7.1.36.3.2 description

interface-config-vlan-instance

Defines this VLAN interface's description. Use this command to provide additional information about the VLAN.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
description <WORD>
```

Parameters

- `description <WORD>`

description <WORD>	Configures a description for this VLAN interface (should not exceed 64 characters in length) • <WORD> – Specify a description unique to the VLAN's specific configuration, to help differentiate it from other VLANs with similar configurations.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#description "This VLAN
interface is configured for the Sales Team"

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  description "This VLAN interface is configured for the Sales Team"
  crypto map map1
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

Related Commands

no	Removes the VLAN interface description

7.1.36.3.3 dhcp

interface-config-vlan-instance

Enables inclusion of optional fields (client identifier) in DHCP client requests. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp client include client-identifier
```

Parameters

- `dhcp client include client-identifier`

dhcp client include client-identifier	Enables inclusion of client identifier in DHCP client requests

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#dhcp client include
client-identifier

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  dhcp client include client-identifier
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

Related Commands

no	Disables inclusion of client identifier in DHCP client requests

7.1.36.3.4 dhcp-relay-incoming

interface-config-vlan-instance

Allows an onboard DHCP server to respond to relayed DHCP packets. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp-relay-incoming
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#dhcp-relay-incoming

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  description "This VLAN interface is configured for the Sales Team"
  crypto map map1
  dhcp-relay-incoming
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

Related Commands

no	Disables or reverts interface VLAN settings to their default

7.1.36.3.5 ip

interface-config-vlan-instance

Configures the VLAN interface's IP settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip [address|dhcp|helper-address|nat|ospf]

ip helper-address <IP>

ip address [<IP/M>|<NETWORK-ALIAS-NAME>|dhcp|zeroconf]
ip address [<IP/M>|<NETWORK-ALIAS-NAME>|zeroconf] {secondary}
ip address dhcp

ip dhcp client request options all

ip nat [inside|outside]

ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|
priority]

ip ospf authentication [message-digest|null|simple-password]
ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]
ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]
ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]
```

Parameters

- `ip helper-address <IP>`

helper-address <IP>	Enables DHCP and BOOTP requests forwarding for a set of clients. Configure a helper address on the VLAN interface connected to the client. The helper address should specify the address of the BOOTP or DHCP servers to receive the requests. If you have multiple servers, configure one helper address for each server. • <IP> – Specify the IP address of the DHCP or BOOTP server.

- `ip address [<IP/M>|<NETWORK-ALIAS-NAME>|zeroconf] {secondary}`

address	Sets the VLAN interface's IP address
<IP/M>	Specifies the interface IP address in the A.B.C.D/M format • secondary – Optional. Sets the specified IP address as a secondary address
<NETWORK-ALIAS-NAME>	Uses a pre-defined network alias to provide this VLAN interface's IP address. Specify the network alias name. • secondary – Optional. Sets the network-alias provided IP address as the secondary address
zeroconf {secondary}	Uses *Zero Configuration Networking* (zeroconf) to generate an IP address for this interface Contd..

	Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. • secondary – Optional. Sets the generated IP address as a secondary address

- `ip address dhcp`

address	Sets the VLAN interface's IP address
dhcp	Uses a DHCP client to obtain an IP address for this VLAN interface

- `ip dhcp client request options all`

dhcp	Uses a DHCP client to configure a request on this VLAN interface
client	Configures a DHCP client
request	Configures DHCP client request
options	Configures DHCP client request options
all	Configures all DHCP client request options

- `ip nat [inside|outside]`

nat [inside|outside]	Defines NAT settings for the VLAN interface. NAT is disabled by default. • inside – Enables NAT on the inside interface. The inside network is transmitting data over the network to the intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. • outside – Enables NAT on the outside interface. Packets passing through the NAT on the way back to the managed LAN are searched against the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.

- `ip ospf authentication [message-digest|null|simple-password]`

ospf authentication	Configures OSPF authentication scheme. Options are message-digest, null, and simple-password.
message-digest	Configures md5 based authentication
null	No authentication required
simple-password	Configures simple password based authentication

- `ip ospf authentication-key simple-password [0 <WORD>|2 <WORD>]`

ospf authentication-key	Configures an OSPF authentication key
simple-password [0 <WORD>|2 <WORD>]	Configures a simple password OSPF authentication key • 0 <WORD> – Configures clear text key • 2 <WORD> – Configures encrypted key

- `ip ospf [bandwidth <1-10000000>|cost <1-65535>|priority <0-255>]`

bandwidth <1-10000000>	Configures bandwidth for the physical port mapped to this layer 3 interface • <1-10000000> – Specify the bandwidth from 1 - 10000000.

cost <1-65535>	Configures OSPF cost • <1-65535> – Specify OSPF cost value from 1 - 65535.
priority <0-255>	Configures OSPF priority • <0-255> – Specify OSPF priority value from 0 - 255.

- `ip ospf message-digest-key key-id <1-255> md5 [0 <WORD>|2 <WORD>]`

ospf message-digest	Configures message digest authentication parameters
key-id <1-255>	Configures message digest authentication key ID from 0 - 255
md5 [0 <WORD>|2 <WORD>]	Configures md5 key • 0 <WORD> – Configures clear text key • 2 <WORD> – Configures encrypted key

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#ip address 10.0.0.1/8

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#ip nat inside

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#ip helper-address
172.16.10.3

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#ip dhcp client request
options all

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  description "This VLAN interface is configured for the Sales Team"
  ip address 10.0.0.1/8
  ip dhcp client request options all
  ip helper-address 172.16.10.3
  ip nat inside
  crypto map map1
  dhcp-relay-incoming
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

Related Commands

no	Removes or resets IP settings on this interface

7.1.36.3.6 ipv6

interface-config-vlan-instance

Configures the VLAN interface's IPv6 settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 [accept|address|dhcp|enable|enforce-dad|mtu|redirects|request-dhcpv6-
options|router-advertisements]

ipv6 accept ra {(no-default-router|no-hop-limit|no-mtu)}

ipv6 address [<IPv6/M>|autoconfig|eui-64|link-local|prefix-from-provider]

ipv6 address [<IPv6/M>|autoconfig]
ipv6 address eui-64 [<IPv6/M>|prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-
LENGTH>]
ipv6 address prefix-from-provider <WORD> <HOST-PORTION/LENGTH>
ipv6 address link-local <LINK-LOCAL-ADD>

ipv6 dhcp [client [information|prefix-from-provider <WORD>]|relay destination
<DEST-IPv6-ADD>]

ipv6 [enable|enforce-dad|mtu <1280-1500>|redirects|request-dhcpv6-options]

ipv6 router-advertisements [prefix <IPv6-PREFIX>|prefix-from-provider <WORD>] {no-
autoconfig|off-link|site-prefix|valid-lifetime}
```

Parameters

- `ipv6 accept ra {(no-default-router|no-hop-limit|no-mtu)}`

ipv6 accept ra	Enables processing of *router advertisements* (RAs) on this VLAN interface. This option is enabled by default. When enabled, IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to the request with a router advertisement packet containing Internet layer configuration parameters.
no-default-router	Optional. Disables inclusion of routers on this interface in the default router selection process. This option is disabled by default.
no-hop-limit	Optional. Disables the use of RA advertised hop-count value on this interface. This option is disabled by default.
no-mtu	Optional. Disables the use of RA advertised MTU value on this interface. This option is disabled by default.

- `ipv6 address [<IPv6/M>|autoconfig]`

ipv6 address [<IPv6/M>|autoconfig]	Configures IPv6 address related settings on this VLAN interface • <IPv6> – Specify the non-link local static IPv6 address and prefix length of the interface in the X:X::X:X/M format. • autoconfig – Enables stateless auto-configuration of IPv6 address, based on the prefixes received from RAs (with auto-config flag set). These prefixes are used to auto-configure the IPv6 address. This option is enabled by default. Use the *no > ipv6 > address > autoconfig* command to negate the use of prefixes received in RAs.

- `ipv6 address eui-64 [<IPv6/M>|prefix-from-provider <WORD> <IPv6-PREFIX/PREFIX-LENGTH>]`

ipv6 address eui-64	Configures the IPv6 prefix and prefix length. This prefix is used to auto-generate the static IPv6 address (for this interface) in the modified *Extended Unique Identifier* (EUI)-64 format. Implementing the IEEE's 64-bit EUI64 format enables a host to automatically assign itself a unique 64-bit IPv6 interface identifier, without manual configuration or DHCP. This is accomplished on a virtual interface by referencing the already unique 48-bit MAC address, and reformatting it to match the EUI-64 specification. In the EUI-64 IPv6 address the prefix and host portions are each 64 bits in length.
<IPv6/M>	Specify the IPv6 prefix and prefix length. This configured value is used as the prefix portion of the auto-generated IPv6 address, and the host portion is derived from the MAC address of the interface. Any bits of the configured value exceeding the prefix-length “M” are ignored and replaced by the host portion derived from the MAC address. For example: Prefix portion provided using this command: ipv6 > address > eui-64 > *2004:b055:15:dead::1111/64.* Host portion derived using the interface’s MAC address (00-15-70-37-FB-5E): *215:70ff:fe37:fb5e* Auto-configured IPv6 address using the above prefix and host portions: *2004:b055:15:dead:215:70ff:fe37:fb5e/64* In this example, the host part “::1111” is ignored and replaced with the modified eui-64 formatted host address.
prefix-from-provider <WORD> <IPv6-PREFIX/ PREFIX-LENGTH>	Configures the “prefix-from-provider” named object and the associated IPv6 prefix and prefix length. This configured value is used as the prefix portion of the auto-generated IPv6 address, and the host portion is derived from the MAC address of the interface. • <WORD> – Specify the IPv6 “prefix-from-provider” object’s name. This is the IPv6 general prefix (32 character maximum) name provided by the Internet service provider. Contd..

	• <IPv6-PREFIX/PREFIX-LENGTH> – Specify the IPv6 address subnet and host parts along with prefix length (site-renumbering). For example: Prefix portion provided using this command: ipv6 > address > eui-64 > *prefix-from-provider > ISP1-prefix > 2002::/64* Host portion derived using the interface's MAC address (00-15-70-37-FB-5E): *215:70ff:fe37:fb5e* Auto-configured IPv6 address using the above prefix and host portions: *2002::215:70ff:fe37:fb5e/64*

• `ipv6 address prefix-from-provider <WORD> <HOST-PORTION/LENGTH>]`

ipv6 address	Configures the IPv6 address related settings on this VLAN interface
prefix-from-provider <WORD> <HOST-PORTION/ LENGTH>	Configures the "prefix-from-provider" named object and the host portion of the IPv6 interface address. The prefix derived from the specified "prefix-from-provide" and the host portion (second parameter) are combined together (using the prefix-length of the specified "prefix-from-provide") to generate the interface's IPv6 address. • <WORD> – Provide the "prefix-from-provider" object's name. This is the IPv6 general prefix (32 character maximum) name provided by the service provider. • <HOST-PORTION/LENGTH> – Provide the subnet number, host portion, and prefix length used to form the actual address along with the prefix derived from the "prefix-from-provider" object identified by the <WORD> keyword.

• `ipv6 address link-local <LINK-LOCAL-ADD>`

ipv6 address	Configures the IPv6 address related settings on this VLAN interface
link-local <LINK-LOCAL-ADD>	Configures IPv6 link-local address on this interface. The configured value overrides the default link-local address derived from the interface's MAC address. Use the *no > ipv6 > link-local* command to restore the default link-local address derived from MAC address. It is mandatory for an IPv6 interface to always have a link-local address.

• `ipv6 dhcp [client [information|prefix-from-provider <WORD>]|relay destination <DEST-IPv6-ADD>]`

ipv6 dhcp client [information| prefix-from-provider <WORD>]	Configures DHCPv6 client-related settings on this VLAN interface • information – Configures stateless DHCPv6 client on this interface. When enabled. the device can request configuration information from the DHCPv6 server using stateless DHCPv6. This option is disabled by default. • prefix-from-provider – Configures prefix-delegation client on this interface. Enter the IPv6 general prefix (32 character maximum) name provided by the service provider. This option is disabled by default.

relay destination <DEST-IPv6-ADD>	Enables DHCPv6 packet forwarding on this VLAN interface • destination – Forwards DHCPv6 packets to a specified DHCPv6 relay • <DEST-IPv6-ADD> – Specify the destination DHCPv6 relay's address. DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When a DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

• `ipv6 [enable|enforce-dad|mtu <1280-1500>|redirects|request-dhcp-options]`

ipv6	Configures IPv6 settings on this VLAN interface
enable	Enables IPv6 on this interface. This option is disabled by default.
enforce-dad	Enforces *Duplicate Address Detection* (DAD) on wired ports. This option is enabled by default.
mtu <1280-1500>	Configures the *Maximum Transmission Unit* (MTU) for IPv6 packets on this interface • <1280-1500> – Specify a value from 1280 - 1500. The default is 1500.
redirects	Enables ICMPv6 redirect messages sending on this interface. This option is enabled by default.
request-dhcp-options	Requests options from DHCPv6 server on this interface. This option is disabled by default.

• `ipv6 router-advertisements [prefix <IPv6-PREFIX>|prefix-from-provider <WORD>] {no-autoconfig|off-link|site-prefix <SITE-PREFIX>|valid-lifetime}`

ipv6 router-advertisements	Configures IPv6 RA related settings on this VLAN interface
prefix <IPv6-PREFIX>	Configures a static prefix and its related parameters. The configured value is advertised on RAs. • <IPv6-PREFIX> – Specify the IPv6 prefix.
prefix-from-provider <WORD>	Configures a static "prefix-from-provider" named object and its related parameters on this VLAN interface. The configured value is advertised on RAs. • <WORD> – Specify the "prefix-from-provider" named object's name
no-autoconfig	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • no-autoconfig – Optional. Disables the setting of the auto configuration flag in the prefix. When configured, the configured prefixes are not used for IPv6 address generation. The autoconfiguration option is enabled by default. Using no-autoconfig disables it.
off-link	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • off-link – Optional. Disables the setting of the on-link flag in the prefix. The on-link option is enabled by default. Using off-link disables it.
site-prefix <SITE-PREFIX>	This parameter is common to the "general-prefix", "prefix", and "prefix-from-provider" keywords. • site-prefix <SITE-PREFIX> – Configures subnet (site) prefix

valid-lifetime [<30-4294967294>| at|infinite] (preferred-lifetime)	This parameter is common to the “general-prefix”, “prefix”, and “prefix-from-provider” keywords. • valid-lifetime – Configures the valid lifetime for the prefix • preferred-lifetime – Configures preferred lifetime for the prefix • <30-4294967294> – Configures the valid/preferred lifetime in seconds • at – Configures expiry time and date of the valid/preferred lifetime • infinite – Configures the valid/preferred lifetime as infinite

Example

```
rfs6000-81742D(config-profile-test-if-vlan4)#ipv6 enable

rfs6000-81742D(config-profile-test-if-vlan4)#ipv6 accept ra no-mtu

rfs6000-81742D(config-profile-test-if-vlan4)#ipv6 address eui-64 prefix-from-
provider ISP1-prefix 2002::/64

rfs6000-81742D(config-profile-test-if-vlan4)#show context
 interface vlan4
  ipv6 enable
  ipv6 address eui-64 prefix-from-provider ISP1-prefix 2002::/64
  ipv6 accept ra no-mtu
rfs6000-81742D(config-profile-test-if-vlan4)#
```

Related Commands

no	Removes or resets IPv6 settings on this VLAN interface

7.1.36.3.7 no

interface-config-vlan-instance

Negates a command or reverts to defaults. The no command, when used in the Config Interface VLAN mode, negates VLAN interface settings or reverts them to their default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [crypto|description|dhcp|dhcp-relay-incoming|ip|ipv6|shutdown|use]

no dhcp client include client-identifier

no [crypto map|description|dhcp-relay-incoming|shutdown]

no ip [address|dhcp|helper-address|nat|ospf]
no ip [helper-address <IP>|nat]
no ip address {<IP/M> {secondary}|<NETWORK-ALIAS-NAME> {secondary}|dhcp|zeroconf
{secondary}}
no ip dhcp client request options all
no ip ospf [authentication|authentication-key|bandwidth|cost|message-digest-key|
priority]

no ipv6 [accept|address|dhcp|enable|enforce-dad|mtu|redirects|request-dhcpv6-
options|router-advertisement]

no ipv6 [accept ra|enable|enforce-dad|mtu|redirects|request-dhcpv6-options]
no ipv6 address [<IPv6/M>|autoconfig|eui-64|link-local|prefix-from-provider>]
no ipv6 dhcp [client|relay]
no ipv6 router-advertisement [prefix <WORD>|prefix-from-provider <WORD>]

no use [bonjour-gw-discovery-policy>|ip-access-list in|ipv6-access-list in|ipv6-
router-advertisement-policy|url-filter]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts this VLAN interface's settings based on the parameters passed

Example

The following example shows the VLAN interface settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  description "This VLAN interface is configured for the Sales Team"
  ip address 10.0.0.1/8
  ip dhcp client request options all
  ip helper-address 172.16.10.3
  ip nat inside
  crypto map map1
  dhcp-relay-incoming
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#no crypto map
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#no description
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#no dhcp-relay-incoming
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#no ip dhcp client request
options all
```

The following example shows the VLAN interface settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  ip address 10.0.0.1/8
  ip helper-address 172.16.10.3
  ip nat inside
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

7.1.36.3.8 shutdown

interface-config-vlan-instance

Shuts down the selected interface. Use the no shutdown command to enable an interface.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#shutdown

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  ip address 10.0.0.1/8
  ip helper-address 172.16.10.3
  shutdown
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

Related Commands

no	Disables or reverts interface VLAN settings to their default

7.1.36.3.9 use

interface-config-vlan-instance

Associates an IP (IPv4 and IPv6) access list, bonjour-gw-discovery policy, and an IPv6-router-advertisement policy with this VLAN interface

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [bonjour-gw-discovery-policy <POLICY-NAME>|ip-access-list in <IP-ACL-NAME>|ipv6-access-list in <IPv6-ACL-NAME>|ipv6-router-advertisement-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>]
```

Parameters

```
• use [bonjour-gw-discovery-policy <POLICY-NAME>|ip-access-list in <IP-ACL-NAME>|ipv6-access-list in <IPv6-ACL-NAME>|ipv6-router-advertisement-policy <POLICY-NAME>|url-filter <URL-FILTER-NAME>]
```

bonjour-gw-discovery-policy <POLICY-NAME>	Uses an existing Bonjour GW Discovery policy with this VLAN interface. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming over the VLAN interface. • <POLICY-NAME> – Specify the Bonjour GW Discovery policy name (should be existing and configured). For more information on Bonjour GW Discovery policy, see *bonjour-gw-discovery-policy*.
ip-access-list in <IP-ACCESS-LIST-NAME>	Uses a specified IPv4 access list with this interface • in – Applies IPv4 ACL to incoming packets • <IP-ACCESS-LIST-NAME> – Specify the IPv4 access list name.
ipv6-access-list in <IPv6-ACCESS-LIST-NAME>	Uses a specified IPv6 access list with this interface • in – Applies IPv6 ACL to incoming packets • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 access list name.
ipv6-router-advertisement-policy <POLICY-NAME>	Uses an existing IPv6 router advertisement policy with this VLAN interface. • <POLICY-NAME> – Specify the IPv6 router advertisement policy name (should be existing and configured).
url-filter <URL-FILTER-NAME>	Enforces URL filtering on this VLAN interface by associating a URL filter • <URL-FILTER-NAME> – Specify the URL filter name (should be existing and configured).

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#use ip-access-list in
test

rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#show context
 interface vlan8
  ip address 10.0.0.1/8
  use ip-access-list in test
  ip helper-address 172.16.10.3
rfs6000-37FABE(config-profile-default-rfs6000-if-vlan8)#
```

Related Commands

no	Disables or reverts interface VLAN settings to their default

7.1.36.4 interface-config-port-channel-instance

interface

Profiles can utilize customized port channel configurations as part of their interface settings. Existing port channel profile configurations can be overridden as they become obsolete for specific device deployments.

The following example uses the config-profile-testNX9000 instance to configure a port-channel interface:

```
nx9500-6C8809(config-profile-testNX9000)#interface port-channel 1
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
Port Channel Mode commands:
  description      Port description
  duplex           Set duplex to interface
  ip               Internet Protocol (IP)
  ipv6             Internet Protocol version 6 (IPv6)
  no               Negate a command or set its defaults
  port-channel     Portchannel commands
  qos              Quality of service
  remove-override  Remove configuration item override from the device (so
                   profile value takes effect)
  shutdown         Shutdown the selected interface
   spanning-tree    Spanning tree commands
  speed            Configure speed
  switchport       Set switching mode characteristics
  use              Set setting to use

  clrscr           Clears the display screen
  commit           Commit all changes made in this session
  do               Run commands from Exec mode
  end              End current mode and change to EXEC mode
  exit             End current mode and down to previous mode
  help             Description of the interactive help system
  revert           Revert changes
  service          Service Commands
  show             Show running system information
  write            Write running configuration to memory or terminal

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Commands	Description	Reference
description	Configures a brief description for this port-channel interface	*page 7-236*
duplex	Configures the duplex-mode (that is the data transmission mode) for this port-channel interface	*page 7-237*
ip	Configures ARP and DHCP related security parameters on this port-channel interface	*page 7-106*
ipv6	Configures IPv6 related parameters on this port-channel interface	*page 7-239*
no	Removes or reverts to default this port-channel interface's settings	*page 7-242*
shutdown	Shutsdown this port-channel interface	*page 7-244*
spanning-tree	Configures spanning-tree related parameters on this port channel interface	*page 7-245*
speed	Configures the speed at which this port-channel interface receives and transmits data	*page 7-248*
switchport	Configures the packet switching parameters for this port-channel interface	*page 7-249*
use	Configures access controls on this port-channel interface	*page 7-251*

7.1.36.4.1 description

interface-config-port-channel-instance

Configures a brief description for this port channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
description <LINE>
```

Parameters

- `description <LINE>`

description <LINE>	Configures a description for this port-channel interface that uniquely identifies it from other port channel interfaces • <LINE> – Provide a description not exceeding 64 characters in length.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#description "This port
-channel is for enabling dynamic LACP."

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes this port-channel interface's description

7.1.36.4.2 duplex

interface-config-port-channel-instance

Configures the duplex-mode (that is the data transmission mode) for this port channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
duplex [auto|half|full]
```

Parameters

- `duplex [auto|half|full]`

duplex [auto|half|full]	Configures the mode of data transmission as auto, full, or half • auto – Select this option to enable the controller, service platform, or access point to dynamically duplex as port channel performance needs dictate. This is the default setting. • full – Select this option to simultaneously transmit data to and from the port channel. • half – Select this option to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#duplex full

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  duplex full
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Reverts the duplex-mode to the default value (auto)

7.1.36.4.3 ip

interface-config-port-channel-instance

Configures ARP and DHCP related security parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip [arp|dhcp]

ip arp [header-mismatch-validation|trust]

ip dhcp trust
```

Parameters

- `ip arp [header-mismatch-validation|trust]`

ip arp [header-mismatch-validation| trust]	Configures ARP related parameters on this port-channel interface • header-mismatch-validation – Enables a source MAC mismatch check in both the ARP and ethernet headers. This option is enabled by default. • trust – Enables ARP trust on this port channel. If enabled, ARP packets received on this port are considered trusted, and information from these packets is used to identify rogue devices. This option is disabled by default.

- `ip dhcp trust`

`ip dhcp trust`	Enables DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#ip arp trust

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  duplex full
  ip arp trust
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes or reverts to default the ARP and DHCP security parameters configured

7.1.36.4.4 ipv6

interface-config-port-channel-instance

Configures IPv6 related parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 [dhcpv6|nd]

ipv6 dhcpv6 trust

ipv6 nd [header-mismatch-validation|raguard|trust]
```

Parameters

- `ipv6 dhcpv6 trust`

ipv6 dhcpv6 trust	Enables DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. This option is enabled by default.

- `ipv6 nd [header-mismatch-validation|raguard|trust]`

ipv6 nd [header-mismatch-validation| raguard|trust]	Configures IPv6 *neighbor discovery* (ND) parameters • header-mismatch-validation – Enables a mismatch check for the source MAC in both the ND header and link layer options. This option is disabled by default.
raguard	Enables router advertisements or IPv6 redirects from this port. Router advertisements are periodically sent to hosts or are sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is enabled by default.
trust	Enables DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. This option is enabled by default.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#ipv6 nd header-
mismatch-validation

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#ipv6 nd trust

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  duplex full
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  ip arp trust
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes or reverts to default the IPv6 related parameters on this port-channel interface

7.1.36.4.5 port-channel

interface-config-port-channel-instance

Configures client load balancing parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
port-channel load-balance [src-dst-ip|src-dst-mac]
```

Parameters

- `port-channel load-balance [src-dst-ip|src-dst-mac]`

port-channel load-balance [src-dst-ip| src-dst-mac]	Specifies whether port channel load balancing is conducted using a source/ destination IP or a source/destination MAC. • src-dst-ip – Uses a source/destination IP to conduct client load balancing. This is the default setting. • src-dst-mac – Uses a source/destination MAC to conduct client load balancing

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#port-channel load-
balance src-dst-mac

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  duplex full
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  ip arp trust
  port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes or reverts to default the client load balancing parameters on this port-channel interface

7.1.36.4.6 qos

interface-config-port-channel-instance

Configures *Quality of Service* (QoS) related parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
qos trust [802.1p|dscp]
```

Parameters

- `qos trust [802.1p|dscp]`

qos trust [802.1p|dscp]	Configures the following QoS related parameters: • 802.1p – Trusts 802.1p *class of service* (COS) values ingressing on this port channel. This option is enabled by default. • dscp – Trusts IP DSCP QOS values ingressing on this port channel. This option is enabled by default.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#qos trust dscp
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
```

Related Commands

no	Removes the QoS related parameters configured on this port-channel interface

7.1.36.4.7 no

interface-config-port-channel-instance

Removes or reverts to default this port-channel interface's settings

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no beacon [description|duplex|ip|ipv6|port-channel|qos|shutdown|spanning-tree|
speed|switchport|use]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts to default this port-channels interface's settings based on the parameters passed • <PARAMETERS> – Specify the parameters.

Example

The following example shows the port-channel interface's interface settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
description "This port-channel is for enabling dynamic LACP."
  speed 100
  duplex full
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
  use ip-access-list in BROADCAST-MULTICAST-CONTROL
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  spanning-tree portfast
  spanning-tree bpduguard enable
  spanning-tree bpdufilter enable
  spanning-tree mst 1 port-priority 1
  spanning-tree mst 1 cost 20000
  ip arp trust
  port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no duplex
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no ip arp trust
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no ipv6 nd trust
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#no port-channel load-
balance
```

The following example shows the port-channel interface's interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  speed 100
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
  use ip-access-list in BROADCAST-MULTICAST-CONTROL
  ipv6 nd header-mismatch-validation
  spanning-tree portfast
  spanning-tree bpduguard enable
  spanning-tree bpdufilter enable
  spanning-tree mst 1 port-priority 1
  spanning-tree mst 1 cost 20000
  no qos trust dscp
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

7.1.36.4.8 shutdown

interface-config-port-channel-instance

Shutsdown this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

shutdown

Parameters

None

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#shutdown
```

Related Commands

no	Re-enables this port-channel interface

7.1.36.4.9 spanning-tree

interface-config-port-channel-instance

Configures spanning-tree related parameters on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
spanning-tree [bpdufilter|bpduguard|force-version|guard|link-type|mst|port-cisco-interoperability|portfast]

spanning-tree [bpdufilter|bpduguard] [default|disable|enable]

spanning-tree [force-version <0-3>|guard root|portfast|port-cisco-interoperability [disable|enable]]

spanning-tree link-type [point-to-point|shared]

spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]]
```

Parameters

- `spanning-tree [bpdufilter|bpduguard] [default|disable|enable]`

spanning-tree [bpdufilter| bpduguard]	Configures the following BPDU related parameters for this port channel:
	• bpdufilter – Configures the BPDU filtering options. The options are:
	  • default – When selected, makes the bridge BPDU filter value to take effect. This is the default setting.
	  • disable – Disables BPDU filtering
	  • enable – Enables BPDU filtering. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs.
	• bpduguard – Configures the BPDU guard options. The options are
	  • default – When selected, makes the bridge BPDU guard value to take effect. This is the default setting.
	  • disable – Disables guarding this port from receiving BPDUs
	  • enable – Enables BPDU guarding. Enabling the BPDU guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed.
	Execute the portfast command to ensure that fast transitions is enabled on this port channel before configuring BPDU filtering and guarding.

- `spanning-tree [force-version <0-3>|guard root|portfast|port-cisco-interoperability [disable|enable]]`

spanning-tree [force-version <0-3>| guard root| portfast| port-cisco-interoperability [disable|enable]	Configures the following MSTP related parameters for this port channel: • force-version <0-3> – Sets the protocol version to either STP(0), Not Supported(1), RSTP(2) or MSTP(3). MSTP is the default setting • guard root – Enforces root bridge placement. Setting the guard to Root ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. Contd...

	If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position. • portfast – Enables fast transitions on this port channel. When enabled, BPDU filtering and guarding can be enforced on this port. Enable the portfast option and then use the 'bpdufilter' and bpduguard' options to configure BPDU filtering and guarding parameters. This option is disabled by default. • port-cisco-interoperability [disable|enable] – Enables or disables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This option is disabled by default.

- `spanning-tree link-type [point-to-point|shared]`

spanning-tree link-type [point-to-point| shared]	Configures the link type applicable on this port channel. The options are: • point-to-point – Configures a point-to-point link, which indicates the port should be treated as connected to a point-to-point link. Note, a port connected to the wireless device is a point-to-point link. This is the default setting. • shared – Configures a shared link, which indicates this port should be treated as having a shared connection. Note, A port connected to a hub is on a shared link.

- `spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]`

spanning-tree mst <0-15> [cost <1-200000000>| port-priority <0-240>]	Configures the following Multiple Spanning Tree (MST) parameters on this port: • mst <0-15> – Select the MST instance from 0 - 15. • cost <1-200000000> – Configures the port cost from 1 - 200000000. The default path cost depends on the user defined port speed.The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, higher the cost. • port-priority <0-240> – Configures the port priority from 0 - 240. The lower the priority, greater is the likelihood of the port becoming a designated port.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree portfast
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree
bpdufilter enable
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree bpduguard
enable
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree force-
version 3
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree mst 1
cost 20000
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#spanning-tree mst 1
port-priority 1
```

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  duplex full
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  spanning-tree portfast
  spanning-tree bpduguard enable
  spanning-tree bpdufilter enable
  spanning-tree mst 1 port-priority 1
  spanning-tree mst 1 cost 20000
  ip arp trust
  port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes or reverts to default the spanning-tree related parameters configured on this port channel interface

7.1.36.4.10 speed

interface-config-port-channel-instance

Configures the speed at which this port-channel interface receives and transmits data

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
speed [10|100|1000|auto]]]
```

Parameters

- `speed [10|100|1000|auto]`

speed [10|100|1000|auto]	Configure the data receive-transmit speed for this port channel. The options are: • 10 – 10 Mbps • 100 – 100 mbps • 1000 – 1000 Mbps • auto – Enables the system to auto select the speed. This is the default setting. Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. The auto option enables the port-channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful in an environment where different devices are connected and disconnected on a regular basis.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#speed 100

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  speed 100
  duplex full
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  spanning-tree portfast
  spanning-tree bpduguard enable
  spanning-tree bpdufilter enable
  spanning-tree mst 1 port-priority 1
  spanning-tree mst 1 cost 20000
  ip arp trust
  port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes or reverts to default the speed at which this port-channel interface receives and transmits data

7.1.36.4.11 switchport

interface-config-port-channel-instance

Configures the VLAN switching parameters for this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
switchport [access|mode|trunk]

switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]
switchport mode [access|trunk]
switchport trunk [allowed|native]
switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]
switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]
```

Parameters

- `switchport access vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

access vlan [<1-4094>| <VLAN-ALIAS-NAME>]	Configures the VLAN to which this port-channel interface is mapped when the switching mode is set to access. • <1-4094> – Specify the SVI VLAN ID from 1 - 4094. • <VLAN-ALIAS-NAME> – Specify the VLAN alias name (should be existing and configured).

- `switchport mode [access|trunk]`

mode [access|trunk]	Configures the VLAN switching mode over the port channel • access – If selected, the port channel accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. This is the default setting. • trunk – If selected, the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.

- `switchport trunk allowed vlan [<VLAN-ID>|add <VLAN-ID>|none|remove <VLAN-ID>]`

trunk allowed	If configuring the VLAN switching mode as trunk, use this option to configure the VLANs allowed on this port channel. Add VLANs that exclusively send packets over the port channel.
vlan [<VLAN-ID>| add <VLAN-ID>| none| remove <VLAN-ID>	Use this keyword to add/remove the allowed VLANs • <VLAN-ID> – Allows a group of VLAN IDs. Specify the VLAN IDs, can be either a range (55-60) or a comma-separated list (35, 41, etc.) • none – Allows no VLANs to transmit or receive through the layer 2 interface Contd..

	• add <VLAN-ID> – Adds VLANs to the current list
	  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)
	• remove <VLAN-ID> – Removes VLANs from the current list
	  • <VLAN-ID> – Specify the VLAN IDs. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41, etc.)
	Allowed VLANs are configured only when the switching mode is set to “trunk”.

- `switchport trunk native [tagged|vlan [<1-4094>|<VLAN-ALIAS-NAME>]]`

trunk	If configuring the VLAN switching mode as trunk, use this option to configure the native VLAN on this port channel.

native [tagged| vlan [<1-4094>| <VLAN-ALIAS-NAME>]]	Configures the native VLAN ID for the trunk-mode port
	The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
	• tagged – Tags the native VLAN. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header enabling upstream Ethernet devices to know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
	• vlan [<1-4094>|<VLAN-ALIAS-NAME>] – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode.
	  • <1-4094> – Specify a value from 1 - 4094.
	  • <VLAN-ALIAS-NAME> – Specify the VLAN alias name used to identify the VLANs. The VLAN alias should be existing and configured.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#switchport mode trunk

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  speed 100
  duplex full
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  spanning-tree portfast
  spanning-tree bpduguard enable
  spanning-tree bpdufilter enable
  spanning-tree mst 1 port-priority 1
  spanning-tree mst 1 cost 20000
  ip arp trust
  port-channel load-balance src-dst-mac
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes the packet switching parameters configured on this port-channel interface

7.1.36.4.12 use

interface-config-port-channel-instance

Configures access controls on this port-channel interface

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [ip-access-list|ipv6-access-list|mac-access-list] in <IP/IPv6/MAC-ACCESS-LIST-NAME>]]
```

Parameters

```
• use [ip-access-list|ipv6-access-list|mac-access-list] in <IP/IPv6/MAC-ACCESS-LIST-NAME>]
```

use [ip-access-list| ipv6-access-list| mac-access-list] <IP/IPv6/MAC-ACCESS-LIST-NAME>]	Associates an access list controlling the inbound traffic on this port channel. • ip-access-list – Specify the IPv4 specific firewall rules to apply to this profile's port channel configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity. • ipv6-access-list – Specify the IPv6 specific firewall rules to apply to this profile's port channel configuration. IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. • mac-access-list – Specify the MAC specific firewall rules to apply to this profile's port channel configuration. • <IP/IPv6/MAC-ACCESS-LIST-NAME> – Provide the IPv4, IPv6, or MAC access list name based on the option selected. The access list specified should be existing and configured.

Example

```
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#use ip-access-list in
BROADCAST-MULTICAST-CONTROL

nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#show context
 interface port-channel1
  description "This port-channel is for enabling dynamic LACP."
  speed 100
  duplex full
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
  use ip-access-list in BROADCAST-MULTICAST-CONTROL
  ipv6 nd trust
  ipv6 nd header-mismatch-validation
  spanning-tree portfast
--More--
nx9500-6C8809(config-profile-testNX9000-if-port-channel1)#
```

Related Commands

no	Removes the access controls configured on this port-channel interface

7.1.36.5 interface-config-radio-instance

interface

This section documents radio interface configuration parameters applicable only to the access point profiles.

The access point radio interface can be radio1, radio2, or radio3. The AP7161 models contain either a single or a dual radio configuration. Newer AP7161N model access points support single, dual, or triple radio configurations.

To enter the AP/RFS4000 profile > radio interface context, use the following commands:

```
<DEVICE>(config)#profile <AP-TYPE> <PROFILE-NAME>

rfs6000-37FABE(config)#profile ap71xx 71xxTestProfile
rfs6000-37FABE(config-profile-71xxTestProfile)#

rfs6000-37FABE(config-profile-71xxTestProfile)#interface radio 1
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#?
Radio Mode commands:
  adaptivity                  Adaptivity
  aeroscout                   Aeroscout Multicast MAC/Enable
  aggregation                 Configure 802.11n aggregation related parameters
  airtime-fairness            Enable fair access to medium for clients based
                              on their usage of airtime
  antenna-diversity           Transmit antenna diversity for non-11n transmit
                              rates
  antenna-downtilt            Enable ADEPT antenna mode
  antenna-elevation           Specifies the antenna elevation gain
  antenna-gain                Specifies the antenna gain of this radio
  antenna-mode                Configure the antenna mode (number of transmit
                              and receive antennas) on the radio
  assoc-response              Configure transmission parameters for
                              Association Response frames
  association-list            Configure the association list for the radio
  beacon                      Configure beacon parameters
  bridge                      Bridge rf-mode related configuration
  channel                     Configure the channel of operation for this
                              radio
  data-rates                  Specify the 802.11 rates to be supported on this
                              radio
  description                 Configure a description for this radio
  dfs-rehome                  Revert to configured home channel once dfs
                              evacuation period expires
  dynamic-chain-selection     Automatic antenna-mode selection (single antenna
                              for non-11n transmit rates)
  ekahau                      Ekahau Multicast MAC/Enable
  extended-range              Configure extended range
  fallback-channel            Configure the channel to be used for falling
                              back in the event of radar being detected on the
                              current operating channel
  guard-interval              Configure the 802.11n guard interval
  ldpc                        Configure support for Low Density Parity Check
                              Code
  lock-rf-mode                Retain user configured rf-mode setting for this
                              radio
  max-clients                 Maximum number of wireless clients allowed to
                              associate subject to AP limit
  mesh                        Configure radio mesh parameters
  meshpoint                   Enable meshpoints on this radio
  mu-mimo                     Enable multi user MIMO on this radio (selected
                              platforms only)
  no                          Negate a command or set its defaults
```

```
non-unicast                  Configure handling of non-unicast frames
off-channel-scan             Enable off-channel scanning on the radio
placement                    Configure the location where this radio is
                             operating
power                        Configure the transmit power of the radio
preamble-short               Use short preambles on this radio
probe-response               Configure transmission parameters for Probe
                             Response frames
radio-resource-measurement   Configure support for 802.11k Radio Resource
                             Measurement
radio-share-mode             Configure the radio-share mode of operation for
                             this radio
rate-selection               Default or Opportunistic rate selection
remove-override              Negate a command or set its defaults
rf-mode                      Configure the rf-mode of operation for this
                             radio
rifs                         Configure Reduced Interframe Spacing (RIFS)
                             parameters
rts-threshold                Configure the RTS threshold
shutdown                     Shutdown the selected radio interface
smart-rf                     Configure radio specific smart-rf settings
sniffer-redirect             Capture packets and redirect to an IP address
                             running a packet capture/analysis tool
stbc                         Configure Space-Time Block Coding (STBC)
                             parameters
transmit-beamforming         Enable Transmit Beamforming
use                          Set setting to use
wips                         Wireless intrusion prevention related
                             configuration
wireless-client              Configure wireless client related parameters
wlan                         Enable wlans on this radio

clrscr                       Clears the display screen
commit                       Commit all changes made in this session
do                           Run commands from Exec mode
end                          End current mode and change to EXEC mode
exit                         End current mode and down to previous mode
help                         Description of the interactive help system
revert                       Revert changes
service                      Service Commands
show                         Show running system information
write                        Write running configuration to memory or
                             terminal

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

The following table summarizes the radio interface configuration commands:

Commands	Description	Reference
adaptivity	Configures an adaptivity timeout value, in minutes, for avoidance of channels detected with radar or high levels of interference	*page 7-256*
aeroscout	Enables Aeroscout multicast packet forwarding	*page 7-257*
aggregation	Configures 802.11n aggregation parameters	*page 7-258*
airtime-fairness	Enables fair access for clients based on airtime usage	*page 7-261*
antenna-diversity	Transmits antenna diversity for non-11n transmit rates	*page 7-262*
antenna-downtilt	Enables *Advanced Element Panel Technology* (ADEPT) antenna mode	*page 7-263*
antenna-elevation	Configures the antenna's elevation gain. This command is applicable only to the AP7562 model access point	*page 7-264*
antenna-gain	Specifies the antenna gain for the selected radio	*page 7-266*
antenna-mode	Configures the radio antenna mode	*page 7-267*

Commands	Description	Reference
assoc-response	Enables an access point to ignore or respond to an association/ authorization request based on the configured *Received Signal Strength Index* (RSSI) threshold and deny-threshold values	*page 7-268*
association-list	Associates an existing global association list with this radio interface	*page 7-269*
beacon	Configures beacon parameters	*page 7-270*
bridge	Configures client-bridge related parameters, if the selected radio's RF mode is set to bridge	*page 7-272*
channel	Configures a radio's channel of operation	*page 7-278*
data-rates	Specifies the 802.11 rates supported on a radio	*page 7-280*
description	Configures the selected radio's description	*page 7-284*
dfs-rehome	Reverts to configured home channel once *Dynamic Frequency Selection* (DFS) evacuation period expires	*page 7-285*
dynamic-chain-selection	Enables automatic antenna mode selection	*page 7-286*
ekahau	Enables Ekahau multicast packet forwarding	*page 7-287*
extended-range	Configures extended range	*page 7-288*
fallback-channel	Configures the channel to which the radio switches in case of radar detection on the current channel	*page 7-289*
guard-interval	Configures the 802.11n guard interval	*page 7-290*
ldpc	Enables support for *Low Density Parity Check* (LDPC) on the radio interface	*page 7-291*
lock-rf-mode	Retains user configured RF mode settings for the selected radio	*page 7-292*
max-clients	Configures the maximum number of wireless clients allowed to associate with this radio	*page 7-293*
mesh	Configures radio mesh parameters	*page 7-294*
meshpoint	Maps an existing meshpoint to this radio interface	*page 7-296*
mu-mimo	Enables *multi-user multiple input multiple output* (MU-MIMO) support on a radio	*page 7-297*
no	Negates or resets radio interface settings configures on a profile or a device	*page 7-298*
non-unicast	Configures the handling of non unicast frames on this radio	*page 7-301*
off-channel-scan	Enables selected radio's off channel scanning parameters	*page 7-303*
placement	Defines selected radio's deployment location	*page 7-305*
power	Configures the transmit power on this radio	*page 7-306*
preamble-short	Enables the use of short preamble on this radio	*page 7-307*
probe-response	Configures transmission parameters for probe response frames	*page 7-308*
radio-resource-measurement	Enables 802.11k radio resource measurement	*page 7-309*
radio-share-mode	Configures the mode of operation, for this radio, as radio-share	*page 7-310*
rate-selection	Sets the rate selection method to standard or opportunistic	*page 7-311*

Commands	Description	Reference
rf-mode	Configures the radio's RF mode	*page 7-312*
rifs	Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio	*page 7-314*
rts-threshold	Configures the *Request to Send* (RTS) threshold value on this radio	*page 7-315*
service	Enables dynamic control function. This dynamic function controls performance of the radio receiver's *low noise amplifier*s (LNAs).	*page 7-316*
shutdown	Terminates or shuts down selected radio interface	*page 7-317*
smart-rf	Overrides Smart RF channel width setting on the selected radio interface	*page 7-318*
sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool	*page 7-319*
stbc	Configures radio's *Space Time Block Coding* (STBC) mode	*page 7-321*
transmit-beamforming	Enables transmit beamforming on the selected radio interface	*page 7-322*
use	Enables use of an association ACL policy and a radio QoS policy by selected radio interface	*page 7-323*
wips	Enables access point to change its channel of operation in order to terminate rogue devices	*page 7-324*
wireless-client	Configures wireless client parameters on selected radio	*page 7-325*
wlan	Enables a WLAN on selected radio	*page 7-326*

7.1.36.5.1 adaptivity

interface-config-radio-instance

Configures an interval, in minutes, for avoiding channels detected with high levels of interference

As per the *European Telecommunications Standards Institute's* (ETSI) EN 300 328 V1.8.1/ ETSI EN 301 893 V1.7.1 requirements, access points have to monitor interference levels on operating channels, and stop functioning on channels with interference levels exceeding ETSI-specified threshold values.

This command configures the interval for which a channel is avoided on detection of interference, and is applicable only if the channel selection mode is set to ACS, Random, or Fixed.

NOTE: If the channel selection mode is set to Smart, in the Smart-RF policy mode, use the *avoidance-time > [adaptivity|dfs] > <30-3600>* command to specify the interval for which a channel is avoided on detection of high levels of interference or radar. For more information, see *avoidance-time*.

When configured, this feature ensures recovery by switching the radio to a new operating channel. Once adaptivity is triggered, the evacuated channel becomes inaccessible and is available again only after the adaptivity timeout, specified here, expires. In case of fixed channel, the radio switches back to the original channel of operation after the adaptivity timeout expires. On the other hand, ACS-enabled radios continue operating on the new channel even after the adaptivity timeout period expires.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
adaptivity [recovery|timeout <30-3600>]
```

Parameters

- `adaptivity [recovery|timeout <30-3600>]`

adaptivity	Configures adaptivity parameters on the radio. These parameters are: recovery and timeout.
recovery	Enables switching of channels when an access point's radio is in the adaptivity mode. In the adaptivity mode, an access point monitors interference on its set channel and stops functioning when the radio's defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default.
timeout <30-3600>	Configures an adaptivity timeout • <30-3600> – Specify a value from 30 - 3600 minutes. The default is 90 minutes.

Example

```
nx4500-5CFA2B(config-profile-testAP7532-if-radio1)#adaptivity timeout 200

nx4500-5CFA2B(config-profile-testAP7532-if-radio1)#show context
 interface radio1
 adaptivity timeout 200
nx4500-5CFA2B(config-profile-testAP7532-if-radio1)#
```

Related Commands

no	Removes the configured adaptivity timeout value and disables adaptivity recovery

7.1.36.5.2 aeroscout

interface-config-radio-instance

Enables Aeroscout multicast packet forwarding. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP6532, AP7502, AP7522

Syntax

```
aeroscout [forward ip <IP> port <0-65535>|mac <MAC>]
```

Parameters

- `aeroscout [forward ip <IP> port <0-65535>|mac <MAC>]`

aeroscout	Enables Aeroscout packet forwarding and configures the packet forwarding parameters

forward ip <IP> port <0-65535>	Configures the following Aeroscout locationing engine details:
	• ip – Configures Aeroscout engine's IP address
	  • <IP> – Specify the Aeroscout engine's IP address. When specified, the AP forwards Aeroscout beacons directly to the Aeroscout locationing engine without proxying through the controller or RF Domain manager.
	• port – Configures the port on which the Aeroscout engine is reachable
	  • <0-65535> – Specify the port number from 0 - 65535.

mac <MAC>	Configures the multicast MAC address to forward the Aeroscout packets • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format. The default value is 01-0C-CC-00-00-00.

Example

```
nx9500-6C8809(config-profile-ProfileTestAP7532-if-radio2)#aeroscout forward ip
10.233.84.206 port 22

nx9500-6C8809(config-profile-ProfileTestAP7532-if-radio2)#show context
 interface radio2
  aeroscout forward ip 10.233.84.206 port 22
nx9500-6C8809(config-profile-ProfileTestAP7532-if-radio2)#
```

Related Commands

no	Disables Aeroscout packet forwarding

7.1.36.5.3 aggregation

interface-config-radio-instance

Configures 802.11n frame aggregation parameters. Frame aggregation increases throughput by sending two or more data frames in a single transmission. There are two types of frame aggregation: *MAC Service Data Unit* (MSDU) aggregation and *MAC Protocol Data Unit* (MPDU) aggregation. Both modes group several data frames into one large data frame.

Supported in the following platforms:

- Access Points — AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
aggregation [ampdu|amsdu]

aggregation ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing]

aggregation ampdu [rx-only|tx-only|tx-rx|none]

aggregation ampdu max-aggr-size [rx|tx]
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]
aggregation ampdu max-aggr-size tx <2000-65535>

aggregation ampdu min-spacing [0|1|2|4|8|16]

aggregation amsdu [rx-only|tx-rx]
```

Parameters

- `aggregation ampdu [rx-only|tx-only|tx-rx|none]`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures *Aggregate MAC Protocol Data Unit* (AMPDU) frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
tx-only	Supports the transmission of AMPDU aggregated frames only
rx-only	Supports the receipt of AMPDU aggregated frames only
tx-rx	Supports the transmission and receipt of AMPDU aggregated frames (default setting)
none	Disables support for AMPDU aggregation

- `aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
max-aggr-size	Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.

rx [8191|16383|32767|65535]	Configures the maximum limit (in bytes) advertised for received frames • 8191 – Advertises a maximum of 8191 bytes • 16383 – Advertises a maximum of 16383 bytes • 32767 – Advertises a maximum of 32767 bytes • 65535 – Advertises a maximum of 65535 bytes (default setting)

- `aggregation ampdu max-aggr-size tx <2000-65535>`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
max-aggr-size	Configures AMPDU packet size limits. Configure the packet size limit on packets both transmitted and received.
tx <2000-65535>	Configures the maximum size (in bytes) for AMPDU aggregated transmitted frames • <2000-65535> – Sets the limit from 2000 - 65535 bytes. The default is 65535 bytes.

- `aggregation ampdu min-spacing [0|1|2|4|8|16|auto]`

aggregation	Configures 802.11n frame aggregation parameters
ampdu	Configures AMPDU frame aggregation parameters AMPDU aggregation collects Ethernet frames addressed to a single destination. It wraps each frame in an 802.11n MAC header. This aggregation mode is less efficient, but more reliable in environments with high error rates. It enables the acknowledgement and retransmission of each aggregated data frame individually.
mn-spacing [0|1|2|4|8|16]	Configures the minimum gap, in microseconds, between AMPDU frames • 0 – Configures the minimum gap as 0 microseconds • 1 – Configures the minimum gap as 1 microseconds • 2 – Configures the minimum gap as 2 microseconds • 4 – Configures the minimum gap as 4 microseconds • 8 – Configures the minimum gap as 8 microseconds • 16 – Configures the minimum gap as 16 microseconds • auto – Auto configures the minimum gap depending on the platform and radio type (default setting)

- `aggregation amsdu [rx-only|tx-rx]`

aggregation	Configures 802.11n frame aggregation parameters
amsdu	Configures *Aggregated MAC Service Data Unit* (AMSDU) frame aggregation parameters. AMSDU aggregation collects Ethernet frames addressed to a single destination. But, unlike AMPDU, it wraps all frames in a single 802.11n frame.
rx-only	Supports the receipt of AMSDU aggregated frames only (default setting)
tx-rx	Supports the transmission and receipt of AMSDU aggregated frames

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#aggregation ampdu tx-
only

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables 802.11n aggregation parameters

7.1.36.5.4 airtime-fairness

interface-config-radio-instance

Enables fair access to the medium for wireless clients based on their airtime usage (i.e. regardless of whether the client is a high-throughput (802.11n) or legacy client). This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
airtime-fairness {prefer-ht} {weight <1-10>}
```

Parameters

- `airtime-fairness {prefer-ht} {weight <1-10>}`

airtime-fairness	Enables fair access to the medium for wireless clients based on their airtime usage
prefer-ht	Optional. Prioritizes high throughput (802.11n) clients over clients with slower throughput (802.11 a/b/g) and legacy clients
weight <1-10>	Optional. Configures the relative weightage for 11n clients over legacy clients. • <1-10> – Sets a weightage ratio for 11n clients from 1 - 10

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#airtime-fairness prefer-
ht weight 6

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  airtime-fairness prefer-ht weight 6
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables fair access for wireless clients (provides access on a round-robin mode)

7.1.36.5.5 antenna-diversity

interface-config-radio-instance

Configures transmit antenna diversity for non-11n transmit rates

Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
antenna-diversity
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-diversity

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Uses single antenna for non-11n transmit rates

7.1.36.5.6 antenna-downtilt

interface-config-radio-instance

Enables the *Advanced Element Panel Technology* (ADEPT) antenna mode. The ADEPT mode increases the probability of parallel data paths enabling multiple spatial data streams. This option is disabled by default.

Supported in the following platforms:

- Access Point — AP7161

NOTE: This feature is not supported on AP6521, AP6522, AP6532, AP6562, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, and AP8533.

Syntax

```
antenna-downtilt
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-downtilt

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables the ADEPT antenna mode

7.1.36.5.7 antenna-elevation

interface-config-radio-instance

Configures an antenna's elevation gain. Antenna gain is the ratio of an antenna's radiation intensity in a given direction to the intensity produced by a no-loss, isotropic antenna radiating equally in all directions. An antenna's gain along the horizon and at an elevation of 30 degree may vary. The elevation gain is defined as the maximum antenna gain at 30 to 150 degrees above the horizon. If elevation gain is configured, the transmit (TX) power calculations maximize the allowable TX power for an elevation below 30 degree.

Access Points must conform to U.S. *Federal Communications Commission's* (FCC) limitations. FCC has now stipulated a 21dBm *Effective Isotropic Radiated Power* (EIRP) limit for power directed 30 degrees above the horizon.

For Extreme Networks -supplied antennas, compatible with 5.0 GHz on the AP7562 access point, refer to the Antenna Guide for "Elevation Gain" information. If using a third-party antenna, it is required that you obtain the antenna-elevation gain information from the antenna manufacturer.

The elevation gain should be configured if the access point:

- Is deployed outdoors, and
- Is used with a dipole antenna (panel antenna and polarized antenna are for point to point only, and are excluded from this requirement), and
- Is transmitting in the 5.15 - 5.25 GHz *Unlicensed National Information Infrastructure*-1 (UNII-1) band.

Professional installers must complete the following steps to ensure compliance with the FCC rule:

1 Configure the antenna type. For example:

```
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#service antenna-type dipole
```

2 Configure the antenna peak gain. For example:

```
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-gain 7.0
```

3 Configure the antenna placement. For example:

```
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#placement outdoor
```

4 Configure the antenna elevation gain. For example:

```
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-elevation 5.0
```

After the professional installer enters the antenna type, gain, placement, and elevation gain using the CLI as outlined above, the firmware will use this information and hardcoded maximum limits determined during testing (See Annex C in FCC Report #FR4D0448AB) to limit the EIRP below 21dBm for outdoor use in UNII-1 band. The antenna information is provided in the Installation guide and antenna guide.

Supported in the following platforms:

- Access Points — AP7562

Syntax

```
antenna-elevation <-30.0-36.0>
```

NOTE: The antenna elevation gain feature is supported only on the AP7562 model access point.

Parameters

- `antenna-elevation <-30.0-36.0>`

antenna-elevation <-30.0-36.0>	Configures the antenna elevation gain from -30.0 - 36.0 dB. Refer to the antenna specifications for antenna-elevation gain information. The default value is 0 dB.

Example

```
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#antenna-elevation 5.0

ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#show context
interface radio2
  antenna-elevation 5.0
ap7562-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio2)#
```

Related Commands

no	Resets antenna elevation gain to default (0 dB)

7.1.36.5.8 antenna-gain

interface-config-radio-instance

Configures the antenna gain for the selected radio

Antenna gain is the ability of an antenna to convert power into radio waves and vice versa. The access point or wireless controller's *Power Management Antenna Configuration File* (PMACF) automatically configures the access point orwireless controller's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the access point or wireless controller calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. It is recommended that only a professional installer set the antenna gain.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
antenna-gain <0.0-15.0>
```

Parameters

- `antenna-gain <0.0-15.0>`

antenna-gain <0.0-15.0>	Sets the antenna gain from 0.0 - 15.0 dBi. The default is 0.00 dBi.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-gain 12.0

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the radio's antenna gain parameter

7.1.36.5.9 antenna-mode

interface-config-radio-instance

Configures the antenna mode (the number of transmit and receive antennas) on the access point

This command sets the number of transmit and receive antennas on the access point. The 1x1 mode is used for transmissions over just the single -A- antenna, 1xALL is used for transmissions over the -A- antenna and all three antennas for receiving. The 2x2 mode is used for transmissions and receipts over two antennas for dual antenna models. 3x3x3 is used for transmissions and receipts over three antennas for AP81XX models. The default setting is dynamic based on the access point model deployed and its transmit power settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
antenna-mode [1*1|1*ALL|2*2|3*3|default]
```

Parameters

- `antenna-mode [1*1|1*ALL|2*2|default]`

antenna-mode	Configures the antenna mode
1*1	Uses only antenna A to receive and transmit
1*ALL	Uses antenna A to transmit and receives on all antennas
2*2	Uses antennas A and C for both transmit and receive
3*3	Uses antenna A, B, and C for both transmit and receive
default	Uses default antenna settings. This is the default setting.

Usage Guidelines

To support STBC feature on AP7161 profile, the antenna-mode should not be configured to 1*1.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#antenna-mode 2x2

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the radio antenna mode (the number of transmit and receive antennas) to its default

7.1.36.5.10 assoc-response

interface-config-radio-instance

Configures the parameters determining whether the access point ignores or responds to an association/authorization request

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
assoc-response [deny-threshold <1-12>|rssi-threshold <-128--40>]
```

Parameters

- `assoc-response [deny-threshold <1-12>|rssi-threshold <-128--40>]`

assoc-response	Configures the following thresholds, based on which the AP ignores or responds to an association/authorization request: deny-threshold and rssi-threshold. Both these options are disabled by default.
deny-threshold <1-12>	Configures the number of times the AP ignores association/authorization requests, if the RSSI is below the configured RSSI threshold value • <1-12> – Specify a value from 1 - 12. **Note:** The AP always ignores association/authorization requests when deny-threshold *is not* specified and rssi-threshold *is* specified.
rssi-threshold <-128--40>	Configures the RSSI threshold. If the RSSI is lower than the threshold configured here, the AP ignores the association/authorization request. • <128--40> – Specify the RSSI threshold from -128 - -40 dBi.

Example

```
rfs6000-37FABE(config-profile-71XXTestProfile-if-radio1)#assoc-response rssi-
threshold -128

rfs6000-37FABE(config-profile-71XXTestProfile-if-radio1)#show context
 interface radio1
  assoc-response rssi-threshold -128
rfs6000-37FABE(config-profile-71XXTestProfile-if-radio1)#
```

Related Commands

no	Removes the RSSI threshold, based on which an association/authorization request is either ignored or responded.

7.1.36.5.11 association-list

interface-config-radio-instance

Associates an existing global association list with this radio interface

An association ACL is a policy-based *access control list* (ACL) that either prevents or allows wireless clients from connecting to a managed access point radio. An ACL is a sequential collection of permit and deny rules that apply to incoming and outgoing packets. When a packet is received on an interface, the controller, service platform, or access point compares the fields in the packet against the applied ACLs to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified in the ACL, it is dropped.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
association-list global <GLOBAL-ASSOC-LIST-NAME>
```

Parameters

- `association-list global <GLOBAL-ASSOC-LIST-NAME>`

association-list global <GLOBAL-ASSOC-LIST-NAME>	Associates an existing global association list with this radio interface

Example

```
rfs4000-880DA7(config-profile-test-if-radio1)#association-list global test

rfs4000-880DA7(config-profile-test-if-radio1)#show context
 interface radio1
  association-list global test
rfs4000-880DA7(config-profile-test-if-radio1)#
```

Related Commands

no	Removes the global association list associated with this radio interface

7.1.36.5.12 beacon

interface-config-radio-instance

Configures radio beacon parameters

A beacon is a packet broadcasted by adopted radios to keep the network synchronized. Included in a beacon is information, such as the WLAN service area, the radio address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a *Delivery Traffic Indication Message* (DTIM). Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter sensitive.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
beacon [dtim-period|period]

beacon dtim-period [<1-50>|bss]

beacon dtim-period [<1-50>|bss <1-16> <1-50>]

beacon period [50|100|200]
```

Parametersd

- `beacon dtim-period [<1-50>|bss <1-8> <1-50>]`

beacon	Configures radio beacon parameters
dtim-period	Configures the radio DTIM interval. A DTIM is a message that informs wireless clients about the presence of buffered multicast or broadcast data. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive.
<1-50>	Configures a single value to use on the radio. Specify a value between 1 and 50.
bss <1-16> <1-50>	Configures a separate DTIM for a *Basic Service Set* (BSS) on this radio interface • <1-16> – Sets the BSS number from 1 - 16 • <1-50> – Sets the BSS DTIM from 1 - 50. The default is 2.

- `beacon period [50|100|200]`

period [50|100|200]	Configures the beacon period (the interval between consecutive radio beacons) • 50 – Configures 50 K-uSec interval between beacons • 100 – Configures 100 K-uSec interval between beacons (default) • 200 – Configures 200 K-uSec interval between beacons

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#beacon dtim-period bss 2
20
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#beacon period 50

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  beacon period 50
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 20
  beacon dtim-period bss 3 2
  --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Removes the configured beacon parameters

7.1.36.5.13 bridge

interface-config-radio-instance

Configures the client-bridge parameters for radios with *rf-mode* set to *bridge*. When configured as a client bridge, the radio can authenticate and associate to the *Wireless LAN* (WLAN) hosted on the infrastructure access point. After successfully associating with the infrastructure WLAN, the client-bridge access point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, there by providing the clients access to the infrastructure WLAN resources.

NOTE: The radio interface configured to form the client-bridge will not be able to service wireless clients as its *RF mode* is set to *bridge* and not *2.5 GHz* or *5.0 GHz*.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7522, AP7532, AP7562, AP7602, AP7622

Syntax

```
bridge [authentication-type [eap|none]|channel-dwell-time <50-2000>|channel-list
[2.4GHz|5GHz] <LIST>|connect-through-bridges|eap [password <PASSWORD>|type [peap-
mschapv2|tls]|username <USERNAME>]|encryption-type [ccmp|none|tkip]|inactivity-
timeout <0-864000>|keepalive [frame-type [null-data|wnmp]|interval <0-36000>]|
max-clients <1-64>|on-link-loss shutdown-other-radio <1-1800>|on-link-up refresh-
vlan-interface|roam-criteria [missed-beacons <1-60>|rssi-threshold <-128--
40>]|ssid <SSID>|wpa-wpa2 psk [0|2|<LINE>]]
```

Parameters

```
• bridge [authentication-type [eap|none]|channel-dwell-time <50-2000>|channel-
list [2.4GHz|5GHz] <LIST>|connect-through-bridges|eap [password <PASSWORD>]|type
[peap-mschapv2|tls]|username <USERNAME>]|encryption-type [ccmp|none|tkip]|
inactivity-timeout <0-864000>|keepalive [frame-type [null-data|wnmp]|interval <0-
36000>]|max-clients <1-64>|on-link-loss shutdown-other-radio <1-1800>|on-link-up
refresh-vlan-interface|roam-criteria [missed-beacons <1-60>|rssi-threshold <-128-
-40>]|ssid <SSID>|wpa-wpa2 psk [0|2|<LINE>]]
```

bridge	Configures client-bridge related parameters on the selected radio Prior to configuring the client-bridge parameters, set the radio's rf-mode to bridge.
authentication-type [eap|none]	Configures the authentication method used to authenticate with the infrastructure WLAN. The authentication mode specified here should be the same as that configured on the infrastructure WLAN. The options are: • eap – Uses EAP authentication (802.1X). If using EAP, use the 'eap' keyword to configure EAP related parameters. • none – Uses no authentication. This is the default setting.
channel-dwell-time <50-2000>	Configures the channel-dwell time in milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the channel-list) when scanning for an infrastructure WLAN. • <50-2000> – Specify a value from 50 -2000 milliseconds. The default is 150 milliseconds.

channel-list [2.4GHz|5GHz] <LIST>	Configures the list of channels the radio scans when scanning for an infrastructure WLAN access point to associate • 2.4GHz <LIST> – Configures a list of channels for scanning across all the channels in the 2.4GHz radio band • 5GHz <LIST> – Configures a list of channels for scanning across all the channels in the 5.0 GHz radio band The following parameter is common to both of the 2.5 GHz and 5.0 GHz bands: • <LIST> – Provide the list of channels separated by commas.
connect-through-bridges	Enables the client-bridge access point radio to connect to an infrastructure WLAN, which already has other client-bridge radios associated with it. The client-bridge access points, in this scenario, are said to be daisy chained together.
eap [password [<PASSWORD>]| type [peap-mschapv2| tls]|username <UESERNAME>]	Configures EAP authentication parameters if the authentication mode is set as EAP • password [0|2|<PASSWORD>] – Configures the EAP authentication password to use with the infrastructure WLAN. The password type depends on the EAP authentication type configured. PEAP-MSCHAPv2 - PEAP password TLS – PKCS #12 certificate secret Use of EAP-TLS authentication is recommended since it is stronger than PEAP-MSCHAPv2. • <PASSWORD> – Enter the password. • type [peap-mschapv2|tls] – Configures the EAP authentication type as: • PEAP-MSCHAPv2 – Configures the EAP authentication type as PEAP-MSCHAPv2. This is the default setting. • TLS – Configures the EAP authentication type as TLS • username <USERNAME> – Configures the EAP authentication user name to use with the infrastructure WLAN. • <USERNAME> – Specify the EAP username. PEAP-MSCHAPv2 – PEAP username (example client-bridge) TLS – Username in the CN field of the installed PKCS #12 client certificate (example client-bridge@example.com)
encryption-type [ccmp|none|tkip]	Configures the encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are: • ccmp – Uses WPA/WPA2 CCMP encryption • none – Uses no encryption method. This is the default setting. • tkip – Uses WPA/WPA2 TKIP encryption If using CCMP or TKIP, use the 'wpa2-wpa2' keyword to configure the *pre-shared key* (PSK).
inactivity-timeout <0-864000>	Configures the inactivity timeout for each bridge MAC address. This is the time for which the client-bridge access point waits before deleting a MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a MAC address for 120 seconds, it is deleted. The default value is 600 seconds. • <0-864000> – Specify a value from 0 - 864000 seconds. The default is 600 seconds.

keepalive [frame-type [null-data|wnmp]| interval <0-36000>]	Configures the keep-alive frame type and interval • frame-type – Configures the keepalive frame type exchanged between the client-bridge access point and the infrastructure access point/controller. The options are: • null-data – Transmits 802.11 NULL data frames. This is the default setting. • wnmp – Transmits *Wireless Network Management Protocol* (WNMP) multicast packet • interval <0-36000> – Configures the interval, in seconds, between two successive keep-alive frame transmission. • <0-36000> – Specify a value from 0 - 36000 seconds. The default is 300 seconds.
max-clients <1-64>	Configures the maximum number of clients that the client-bridge AP can support • <1-14> – Specify a value from 1 - 64. The default is 64.
on-link-loss shutdown-other-radio <1-1800>	Configures the radio-link behaviour when the link between the client-bridge and infrastructure access points is lost. • shutdown-other-radio – Enables shutting down of the *non-client bridge* radio (this is the radio to which wireless-clients associate) when the link between the client-bridge and infrastructure access points is lost. When enabled, clients associated with the non-client bridge radio are pushed to search for and associate with other access points having backhaul connectivity. This option is disabled by default. • <1-1800> – If enabling this option, use this parameter to configure the time, in seconds, for which the non-client bridge radio is shut down. Specify a value from 1 - 1800 seconds.
on-link-up refresh-vlan-interface	Configures the radio-link behaviour when the link between the client-bridge and infrastructure access points comes up. • refresh-vlan-interface – Enables the SVI to refresh on re-establishing client bridge link to infrastructure Access Point. And, if using a DHCP assigned IP address, causes a DHCP renew. This option is enabled by default.
roam-criteria [missed-beacons <1-60>| rssi-threshold <-128--40>]	Configures the following roaming criteria parameters • missed-beacons <1-60> – Configures the missed beacon interval from 0 - 60 seconds.This is the time for which the client-bridge Access Point waits for after missing a beacon from the associated infrastructure Access Point, before roaming to another infrastructure Access Point. For example, if the missed-beacon time is set to 30 seconds, and if more than 30 seconds have passed since the last received beacon, from the associated infrastructure Access Point, the client-bridge Access Point resumes scanning for another infrastructure Access Point. The default value s 20 seconds. • <1-60> – Specify a value from 1 - 60 seconds. The default is 20 seconds. • rssi-threshold <-128--40> – Configures the minimum signal strength, received from target AP, for the bridge connection to be maintained before roaming • <-128--40> – Specify a value from -128 - -40 dBm. If the RSSI value of signals received from the infrastructure access point falls below the specified value, the client-bridge access point resumes scanning for another infrastructure access point. The default is -75 dBm.
ssid <SSID>	Configures the infrastructure WLAN SSID the client bridge connects to • <SSID> – Specify the SSID.

wpa-wpa2 psk [0|2|<LINE>]	Configures the encryption *pre-shared key* (PSK) to use with the infrastructure WLAN • 0 – Configures clear text psk • 2 – Configures encrypted psk • <LINE> – Enter the key **Note:** Pre-shared keys are valid only when the *authentication-type* is set to *none* and the *encryption-type* is set to *tkip* or *ccmp*. **Note:** The PSK should be 8 - 32 characters in length.

Usage Guidelines EAP Authentication

Use the following commands to view client-bridge configuration:

1 show > wireless > bridge > config
Shows the current client bridge configuration.

2 show > wireless > bridge > candidate-ap
Shows the available infrastructure WLAN candidates that are found during the last scan.

3 show > wireless > bridge > host
Shows the wired/wireless clients that are being bridged.

4 show > wireless > bridge > statistics > rf
Shows the client bridge RF statistics.

5 show > wireless > bridge > statistics > traffic

Shows the client bridge traffic statistics.

6 show > wireless > bridge > certificate > status
Shows the client bridge authentication certificate status.

Example

The following examples show the basic parameters that need to be configured on the Infrastructure and the client-bridge APs in order to enable the client-bridge AP to associate with the Infrastructure WLAN. Note, in this example, the authentication mode is set to 'none' and the encryption-type is set to 'ccmp'. The authentication and encryption modes used will vary as per requirement.

1 Configuring the Infrastructure WLAN:

```
InfrastrNOC(config)#wlan cb-psk
InfrastrNOC(config-wlan-cb-psk)#ssid cb-psk
InfrastrNOC(config-wlan-cb-psk)#encryption-type ccmp
InfrastrNOC(config-wlan-cb-psk)#wpa-wpa2 psk extreme@123
InfrastrNOC(config-wlan-cb-psk)#authentication-type none

InfrastrNOC(config)#show running-config wlan cb-psk
wlan cb-psk
  ssid cb-psk
  bridging-mode local
  encryption-type ccmp
  authentication-type none
  wpa-wpa2 psk 0 extreme@123

InfrastrNOC(config)#
```

2 Associating the 'cb-psk' WLAN to the Infrastructure AP's radio.

```
Infra7131-5F5078(config-device-B4-C7-99-5F-50-78-if-radio2)#wlan cb-psk
```

```
Infra7131-5F5078(config-device-B4-C7-99-5F-50-78)#show context
ap71xx B4-C7-99-5F-50-78
 use profile default-ap71xx
 use rf-domain default
 hostname Infra7131-5F5078
 country-code us
 channel-list 5GHz 149,153,157,161,165
 trustpoint radius-ca TP-infra-AP
 trustpoint radius-server TP-infra-AP
 use radius-server-policy cb-rad-srvr
 interface radio2
  rf-mode 5GHz-wlan
  channel smart
  power smart
  data-rates default
  wlan cb-psk bss 1 primary
  no preamble-short
  bridge ssid cb-psk
  bridge encryption-type ccmp
  bridge authentication-type none
  bridge wpa-wpa2 psk 0 extreme@123
 logging on
 logging console debugging
 controller host 192.168.9.31
Infra7131-5F5078(config-device-B4-C7-99-5F-50-78)#
```

3 Confirming the Infrastructure AP's radio interface status.

```
Infra7131-5F5078(config)#show wireless radio
-------------------------------------------------------------------------------
----------------
RADIO               RADIO-MAC            RF-MODE        STATE       CHANNEL
POWER #CLIENT
-------------------------------------------------------------------------------
----------------
Infra7131-5F5078:R1  B4-C7-99-5E-51-40 2.4GHz-wlan          Off   N/A (  smt)
0 (smt)       0
Infra7131-5F5078:R2  B4-C7-99-5E-1A-40   5GHz-wlan           On   165 (  165)
17 (smt)       2
-------------------------------------------------------------------------------
----------------
Total number of radios displayed: 2
Infra7131-5F5078(config)#
```

4 Configuring the client-bridge AP's radio parameters.

```
ap7532-85B274(config-device-84-24-8D-85-B2-74-if-radio2)#bridge ssid cb-psk
ap7532-85B274(config-device-84-24-8D-85-B2-74-if-radio2)#bridge encryption-
type
ccmp
ap7532-85B274(config-device-84-24-8D-85-B2-74-if-radio2)#bridge
authentication-t
ype none
ap7532-85B274(config-device-84-24-8D-85-B2-74-if-radio2)#wpa-wpa2 psk
extreme@123

ap7532-85B274(config-device-84-24-8D-85-B2-74-if-radio2)#show context
 interface radio2
  bridge ssid cb-psk
  bridge encryption-type ccmp
  bridge authentication-type none
bridge wpa-wpa2 psk 0 extreme@123
ap7532-85B274(config-device-84-24-8D-85-B2-74-if-radio2)#
Note, the SSID, encryption-type, and authentication mode are the same as that
of the Infrastructure WLAN.
```

5 Confirming the client-bridge AP's radio interface status.

```
ap7532-85B274#show wireless radio
```

```
-------------------------------------------------------------------------------
---------------
RADIO               RADIO-MAC             RF-MODE        STATE       CHANNEL
POWER #CLIENT
-------------------------------------------------------------------------------
---------------
ap7532-85B274:R1     84-24-8D-AC-2D-B0 2.4GHz-wlan          Off   N/A (  smt)
0 (smt)       0
ap7532-85B274:R2     84-24-8D-AC-CC-10      bridge           On   165 (  smt)
20 (smt)       0
-------------------------------------------------------------------------------
---------------
Total number of radios displayed: 2

================================================

ap7532-85B274(config-device-84-24-8D-85-B2-74)#
```

6 Viewing the *candidate-ap* (connected Infrastructure AP's) details *on the client-bridge AP*.

```
ap7532-85B274(config-device-84-24-8D-85-B2-74)#show wireless bridge candidate-
ap

84-24-8D-AC-CC-10 Client Bridge Candidate APs:
  AP-MAC             BAND    CHANNEL SIGNAL(dbm) STATUS
  B4-C7-99-5E-1A-40  5 GHz   165     -21         selected

Total number of candidates displayed: 1
Total number of client bridges displayed: 1

=======================================================
ap7532-85B274(config-device-84-24-8D-85-B2-74)#
```

7 Viewing the bridge host details on the *client-bridge AP*.

```
ap7532-85B274(config-device-84-24-8D-85-B2-74)#show wireless bridge hosts
-------------------------------------------------------------------------------
HOST MAC             BRIDGE MAC         IP             BRIDGING STATUS ACTIVITY
                                                                    (sec ago)
-------------------------------------------------------------------------------
84-24-8D-85-B2-74    84-24-8D-AC-CC-10 10.1.0.249      UP            00:00:07
-------------------------------------------------------------------------------
Total number of hosts displayed: 1
ap7532-85B274(config-device-84-24-8D-85-B2-74)#
```

Related Commands

no	Removes or resets this client-bridge settings

7.1.36.5.14 channel

interface-config-radio-instance

Configures a radio's channel of operation

Only a trained installation professional should define the radio channel. Select Smart for the radio to scan non-overlapping channels listening for beacons from other access points. After the channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it selects the channel with the lowest average power level.

NOTE: Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, and appear only when using an AP8232, and are unique to the 80 MHz band.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
channel [smart|acs|random|1|2|3|4|-------]
```

Parameters

- `channel [smart|acs|random|1|2|3|4|-------]`

channel	Configures a radio's channel of operation
[smart|acs|random|1|2|3|4|-------]	Configures a radio's channel of operation. The options are: • smart – Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled). This is the default setting. • acs – Uses *automatic channel selection* (ACS) to assign a channel • random – Randomly assigns a channel • 1 – Channel 1 in 20 MHz mode • 2 – Channel 2 in 20 MHz mode

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#channel 1

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  channel 1
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  ..........................................................................
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  antenna-mode 2x2
  antenna-diversity
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets a radio's channel of operation

7.1.36.5.15 data-rates

interface-config-radio-instance

Configures the 802.11 data rates on this radio

This command sets the rate options depending on the 802.11 protocol and the radio band selected. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5.0 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together.

If dedicating the radio to either 2.4 or 5.0 GHz support, use the *custom* keyword to set a 802.11n *modulation and coding scheme* (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

Data rates are fixed and not user configurable for radios functioning as sensors.

NOTE: Use the rf-mode command to configure a radio's mode of operation.

NOTE: The MCS-1s and MCS-2s options are available for each supported access point. However, the MCS-3s option is only available to the AP8232 model access point, and its ability to provide 3x3x3 MIMO support.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom|mcs]

data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]

data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54|mcs-1s|mcs-2s|mcs-3s|basic-1|
basic-2|basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|basic-24|basic-36|
basic-48|basic-54|basic-mcs-1s]

data-rates mcs qam-only
```

Parameters

- `data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default]`

data-rates	Configures the 802.11 data rates on this radio
b-only	Supports operation in the 802.11b mode only (applicable for 2.4 and 4.9 GHz bands)
g-only	Uses rates that support operation in the 802.11g mode only (applicable for 2.4 and 4.9 GHz bands)
a-only	Uses rates that support operation in the 802.11a mode only (applicable for 5.0 GHz band only)

bg	Uses rates that support 802.11b and 802.11g wireless clients (applicable for 2.4 and 4.9 GHz bands)
bgn	Uses rates that support 802.11b, 802.11g, and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)
gn	Uses rates that support 802.11g and 802.11n wireless clients (applicable for 2.4 and 4.9 GHz bands)
an	Uses rates that support 802.11a and 802.11n wireless clients (applicable for 5.0 GHz band only)
default	Enables the default data rates according to the radio's band of operation

```
• data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54||mcs-1s|mcs-2s|mcs-3s|
basic-1|basic-2|basic-5.5|basic-6|basic-9|basic-11|basic-12|basic-18|basic-24|
basic-36|basic-48|basic-54|basic-mcs-1s]
```

data-rates	Configures the 802.11 data rates on this radio
custom	Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it's used as a basic rate (For example, 'data-rates custom basic-1 basic-2 5.5 11') • 1 – 1-Mbps • 2 – 2-Mbps • 5.5 – 5.5-Mbps • 6 – 6-Mbps • 9 – 9-Mbps • 11 – 11-Mbps • 12 – 12-Mbps • 18 – 18-Mbps • 24 – 24-Mbps • 36 – 36-Mbps • 48 – 48-Mbps • 54 – 54-Mbps • mcs-1s – Applicable to 1-spatial stream data rates • mcs-2s – Applicable to 2-spatial stream data rates • mcs-3s – Applicable to 3-spatial stream data rates (supported only on AP8232 for the MIMO feature) • basic-1 – Basic 1-Mbps • basic-2 – Basic 2-Mbps • basic-5.5 – Basic 5.5-Mbps • basic-6 – Basic 6-Mbps • basic-9 – Basic 9-Mbps • basic-11 – Basic 11-Mbps • basic-12 – Basic 12-Mbps • basic-18 – Basic 18-Mbps • basic-24 – Basic 24-Mbps • basic-36 – Basic 36-Mbps Contd..

	• basic-48 – Basic 48-Mbps • basic-54 – Basic 54-Mbps • basic-mcs-1s – Modulation and Coding Scheme data rates for 1 Spatial Stream **Note:** Refer to the *Usage Guidelines (Supported data rates)* section for 802.11an and 802.11ac MCS detailed dates rates for both with and without *short guard intervals* (SGI).

- `data-rates mcs qam-only`

data-rates	Configures the 802.11 data rates on this radio
mcs qam-only	Configures supports for MCS QAM data rates only

Usage Guidelines (Supported data rates)

The following table defines the 802.11n MCS for MCS 1 streams, both with and without SGI:

MCS-1Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
0	1	6.5	7.2	13.5	15
1	1	13	14.4	27	30
2	1	19.5	21.7	40.5	45
3	1	26	28.9	54	60
4	1	39	43.4	81	90
5	1	52	57.8	108	120
6	1	58.5	65	121.5	135
7	1	65	72.2	135	150

The following table defines the 802.11n MCS for MCS 2 streams, both with and without SGI:

MCS-2Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
0	2	13	14.4	27	30
1	2	26	28.9	54	60
2	2	39	43.4	81	90
3	2	52	57.8	108	120
4	2	78	86.7	162	180
5	2	104	115.6	216	240
6	2	117	130	243	270
7	2	130	144.4	270	300

The following table defines the 802.11n MCS for MCS 3 streams, both with and without SGI:

MCS-3Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	20 MHz With SGI
0	3	19.5	21.7	40.5	45
1	3	39	43.3	81	90
2	3	58.5	65	121.5	135
3	3	78	86.7	162	180
4	3	117	130.7	243	270
5	3	156	173.3	324	360
6	3	175.5	195	364.5	405
7	3	195	216.7	405	450

The following table defines the 802.11ac MCS rates (theoretical throughput for single spatial streams) both with and without SGI:

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz No SGI
0	6.5	7.2	13.5	15	29.3	32.5
1	13	14.4	27	30	58.5	65
2	19.5	21.7	40.5	45	87.8	97.5
3	26	28.9	54	60	117	130
4	39	43.3	81	90	175.5	195
5	52	57.8	108	120	234	260
6	58.5	65	121.5	135	263.3	292.5
7	65	72.2	135	150	292,5	325
8	78	86.7	162	180	351	390
9	N/A	N/A	180	200	390	433.3

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#data-rates b-only

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  ..........................................................
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the 802.11 data rates on a radio
rf-mode	Configures the radio's RF mode of operation

7.1.36.5.16 description

interface-config-radio-instance

Configures the selected radio's description that helps differentiate it from other radios with similar configurations

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
description <WORD>
```

Parameters

- `description <WORD>`

description <WORD>	Provide a description for the selected radio (should not exceed 64 characters in length).

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#description "Primary
radio to use"

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Removes a radio's description

7.1.36.5.17 dfs-rehome

interface-config-radio-instance

Reverts to configured home channel once the *Dynamic Frequency Selection* (DFS) evacuation period expires

NOTE: This option is applicable only if the radio's RF mode is set to '5GHz-wlan'.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
dfs-rehome {holdtime <30-3600>}
```

Parameters

- `dfs-rehome {holdtime <30-3600>}`

dfs-rehome {holdtime <30-3600>}	Enables the radio to revert to the configured home channel once the DFS evacuation period expires • holdtime – Optional. Specifies the duration, in minutes, to stay in the new channel • <30-3600> – Specify the holdtime from 30 - 3600 minutes. The default is 90 minutes.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#dfs-rehome holdtime 500

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  dfs-rehome holdtime 500
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Stays on DFS elected channel after evacuation period expires

7.1.36.5.18 dynamic-chain-selection

interface-config-radio-instance

Enables automatic antenna mode selection. When enabled, the radio can dynamically change the number of transmit chains used (uses a single chain/antenna for frames at non-11n transmit rates). This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
dynamic-chain-selection
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#dynamic-chain-selection
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Uses the configured transmit antenna mode for all clients

7.1.36.5.19 ekahau

interface-config-radio-instance

Enables Ekahau multicast packet forwarding. When enabled, Ekahau small, battery powered Wi-Fi tags are attached to tracked assets or assets carried by people. Ekahau processes locations, rules, messages, and environmental data and turns the information into locationing maps, alerts and reports.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
ekahau [forward ip <IP> port <0-65535>|mac <MAC>]
```

Parameters

- `ekahau [forward ip <IP> port <0-65535>|mac <MAC>]`

ekahau	Enables Ekahau multicast packet forwarding on this radio
forward ip <IP> port <0-65535>	Enables multicast packet forwarding to the Ekahau engine • ip <IP> – Configures the IP address of the Ekahau engine in the A.B.C.D format • port <0-65535> – Specifies the *TaZman Sniffer Protocol* (TZSP) port on Ekahau engine from 0 - 65535 TZSP is an encapsulation protocol, which is generally used to wrap 802.11 wireless packets.
mac <MAC>	Configures the multicast MAC address to forward the Ekahau multicast packets • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#ekahau forward ip
172.16.10.1 port 3

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
.................................................
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Uses default Ekahau multicast MAC address

7.1.36.5.20 extended-range

interface-config-radio-instance

Enables the extended range capability for AP7161 model access point. When enabled, these access points can exchange signals with their clients at greater distances without being timed out. This option is disabled by default.

Supported in the following platforms:

- Access Point — AP7161

Syntax

```
extended-range <1-25>
```

Parameters

- `extended-range <1-25>`

extended-range <1-25>	Configures extended range on this radio interface from 1 - 25 kilometers. The default is 2 km on 2.4 GHz band and 7 km on 5.0 GHz band.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#extended-range 15

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  extended-range 15
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the extended range to default (7 km for 2.4 GHz and 5 km for 5.0 GHz)

7.1.36.5.21 fallback-channel

interface-config-radio-instance

Configures the channel to which the radio switches in case of radar detection on the current channel

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
fallback-channel [100|100w|100ww|104|104w|104ww|108|108w..............]
```

Parameters

- `fallback-channel [100|100w|100ww|104|104w|104ww|108|108w..............]`

fallback-channel [100|100w|.....]	Configures the fallback channel. This is the channel the radio switches to in case a radar is detected on the radio's current operating channel. • [100|100w|100ww|...] – Select the fall back channel from the available options. **Note:** Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, and appear only when using an AP8232, and are unique to the 80 MHz band.

Example

```
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#fallback-channel 104
NOTE: Functionality is supported only in the US regulatory domain and only a non-
dfs channel can be configured as a fallback channel

nx9500-6C8809(config-profile-testAP81XX-if-radio2)#show context
 interface radio2
  fallback-channel 104
nx9500-6C8809(config-profile-testAP81XX-if-radio2)#
```

Related Commands

no	Removes the fallback-channel configuration

7.1.36.5.22 guard-interval

interface-config-radio-instance

Configures the 802.11n guard interval. A guard interval ensures distinct transmissions do not interfere with one another. It provides immunity to propagation delays, echoes and reflection of radio signals.

The guard interval is the space between transmitted characters. The guard interval eliminates *inter symbol interference* (ISI). ISI which occurs when echoes or reflections from one symbol interferes with another. Adding time between transmissions allows echoes and reflections to settle before the next symbol is transmitted. A shorter guard interval results in shorter symbol times, which reduces overhead and increases data rates by up to 10%.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
guard-interval [any|long]
```

Parameters

- `guard-interval [any|long]`

guard-interval	Configures the 802.11n guard interval
any	Enables the radio to use any short (400nSec) or long (800nSec) guard interval
long	Enables the use of long guard interval (800nSec). This is the default setting.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#guard-interval long

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the 802.11n guard interval to default (long: 800nSec)

7.1.36.5.23 ldpc

interface-config-radio-instance

Enables support for *Low Density Parity Check* (LDPC) codes on the radio interface

LDPC consists of forward error correcting codes that enable error control in data transmission. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
ldpc
```

Parameters

None

Example

```
rfs4000-229D58(config-profile-Test81XX-if-radio1)#ldpc

rfs4000-229D58(config-profile-Test81XX-if-radio1)#show context
 interface radio1
  ldpc
rfs4000-229D58(config-profile-Test81XX-if-radio1)#
```

Related Commands

no	Disables LDPC support

7.1.36.5.24 lock-rf-mode

interface-config-radio-instance

Retains user configured RF mode settings for the selected radio. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
lock-rf-mode
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#lock-rf-mode

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Allows Smart RF to change a radio's RF mode settings

7.1.36.5.25 max-clients

interface-config-radio-instance

Configures the maximum number of wireless clients allowed to associate with this radio

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
max-clients <0-256>
```

Parameters

- `max-clients <0-256>`

max-clients <0-256>	Configures the maximum number of clients allowed to associate with a radio, subject to the access point's limit. Specify a value from 0 - 256. The default is 256. **Note:** The AP6511 and AP6521 model access points can only support 128 clients.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#max-clients 100

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  ..........................................
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-mode 2x2
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the maximum number of wireless clients allowed to associate with a radio

7.1.36.5.26 mesh

interface-config-radio-instance

Use this command to configure radio mesh parameters. A *Wireless Mesh Network* (WMN) is a network of radio nodes organized in a mesh topology. It consists of mesh clients, mesh routers, and gateways.

Each radio setting can have a unique mesh mode and link configuration. This provides a customizable set of connections to other mesh supported radios within the same radio coverage area.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533

Syntax

```
mesh [client|links|portal|preferred-peer|psk]

mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2 <LINE>|
   <LINE>]]
```

Parameters

```
• mesh [client|links <1-6>|portal|preferred-peer <1-6> <MAC>|psk [0 <LINE>|2
<LINE>|<LINE>]]
```

mesh	Configures radio mesh parameters, such as maximum number of mesh links, preferred peer device, client operations, etc.
client	Enables operation as a client Setting the mesh mode to 'client' enables the radio to operate as a mesh client that scans for and connects to mesh portals or nodes that are connected to portals.
links <1-6>	Configures the maximum number of mesh links a radio attempts to create • <1-6> – Sets the maximum number of mesh links from 1 - 6. The default is 6.
portal	Enables operation as a portal Setting the mesh mode to 'portal' turns the radio into a mesh portal. The radio starts beaconing immediately and accepts connections from other mesh nodes, typically the node with a connection to the wired network.
preferred-peer <1-6> <MAC>	Configures a preferred peer device • <1-6> – Configures the priority at which the peer node will be added When connecting to the mesh infrastructure, nodes with lower priority are given precedence over nodes with higher priority. • <MAC> – Sets the MAC address of the preferred peer device (Ethernet MAC of either a AP, wireless controller, or service platform with onboard radios)
psk [0 <LINE>|2 <LINE>| <LINE>]	Configures the pre-shared key. Ensure this key is configured on the access point when staged for mesh, and added to the mesh client and to the portal access point's configuration on the controller or service platform. • 0 <LINE> – Enter a clear text key • 2 <LINE> – Enter an encrypted key • <LINE> – Enter the pre-shared key Pre-shared keys should be 8 - 64 characters in length.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#mesh client

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  mesh client
  beacon period 50
  --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables mesh mode operation of the selected radio

7.1.36.5.27 meshpoint

interface-config-radio-instance

Maps an existing meshpoint to this radio

Use this command to assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533

Syntax

```
meshpoint <MESHPOINT-NAME> {bss <1-16>}
```

Parameters

- `meshpoint <MESHPOINT-NAME> {bss <1-16>}`

meshpoint <MESHPOINT-NAME>	Maps a meshpoint to this radio. Specify the meshpoint name.
bss <1-16>	Optional. Specifies the radio's BSS where this meshpoint is mapped • <1-16> – Specify the BSS number from 1 - 16.

Example

```
rfs6000-37FABE(config-profile-ap71xxTest-if-radio1)#meshpoint test bss 7
rfs6000-37FABE(config-profile-ap71xxTest-if-radio1)#show context
 interface radio1
  meshpoint test bss 7
rfs6000-37FABE(config-profile-ap71xxTest-radio1)#
```

Related Commands

no	Disables meshpoint on the selected radio

7.1.36.5.28 mu-mimo

interface-config-radio-instance

Enables *multi-user multiple input multiple output* (MU-MIMO) support on the selected radio. When enabled, multiple users are able to simultaneously access the same channel using the spatial degrees of freedom offered by MIMO.

Supported in the following platforms:

- Access Points — AP7532, AP7562, AP81XX, AP8232, AP8432, AP8533

Syntax

```
mu-mimo
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-TestAP81xx-if-radio1)#mu-mimo
nx9500-6C8809(config-profile-TestAP81xx-if-radio1)#show context include-factory |
include mu-mimo
  mu-mimo
nx9500-6C8809(config-profile-TestAP81xx-if-radio1)#

ap7532-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#mu-mimo

ap7532-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#show context include-
factory | include mu-mimo
  mu-mimo
ap7532-80C2AC(config-device-84-24-8D-80-C2-AC-if-radio1)#
```

Related Commands

no	Disables mu-mimo on the selected radio

7.1.36.5.29 no

interface-config-radio-instance

Negates a command or resets settings to their default. When used in the profile/device > radio interface configuration mode, the no command disables or resets radio interface settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
no <PARAMETERS>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts this radio interface's settings based on the parameters passed

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs6000-37FABE(config-profile-ap71xxTest-if-radio1)#no ?
  adaptivity                  Adaptivity
  aeroscout                   Use Default Aeroscout Multicast MAC Address
  aggregation                 Configure 802.11n aggregation related parameters
  airtime-fairness            Disable fair access to medium for clients,
                              provide access in a round-robin mode
  antenna-diversity           Use single antenna for non-11n transmit rates
  antenna-downtilt            Reset ADEPT antenna mode
  antenna-elevation           Reset the antenna elevation of this radio to
                              default
  antenna-gain                Reset the antenna gain of this radio to default
  antenna-mode                Reset the antenna mode (number of transmit and
                              receive antennas) on the radio to its default
  assoc-response              Configure transmission parameters for
                              Association Response frames
  association-list            Configure the association list for the radio
  beacon                      Configure beacon parameters
  bridge                      Bridge rf-mode related configuration
  channel                     Reset the channel of operation of this radio to
                              default
  data-rates                  Reset radio data rate configuration to default
  description                 Reset the description of the radio to its
                              default
  dfs-rehome                  Stay on dfs elected channel after evacuation
                              period expires
  dynamic-chain-selection     Use the configured transmit antenna mode for all
                              clients
  ekahau                      Use Default Ekahau Multicast MAC Address
  extended-range              Reset extended range to default
  fallback-channel            Clear the DFS fallback channel for this radio
  guard-interval              Configure default value of 802.11n guard
                              interval (long: 800nSec)
  ldpc                        Configure support for Low Density Parity Check
                              Code
  lock-rf-mode                Allow smart-rf to change rf-mode setting for
                              this radio
  max-clients                 Maximum number of wireless clients allowed to
                              associate
  mesh                        Disable mesh mode operation of the radio
```

```
  meshpoint                    Disable a meshpoint from this radio
  mu-mimo                      Disable multi user MIMO on this radio (selected
                               platforms only)
  non-unicast                  Configure handling of non-unicast frames
  off-channel-scan             Disable off-channel scanning on the radio
  placement                    Reset the placement of the radio to its default
  power                        Reset the transmit power of this radio to
                               default
  preamble-short               Disable the use of short-preamble on this radio
  probe-response               Configure transmission parameters for Probe
                               Response frames
  radio-resource-measurement   Configure support for 802.11k Radio Resource
                               Measurement
  radio-share-mode             Configure the radio-share mode of operation for
                               this radio
  rate-selection               Monotonic rate selection
  rf-mode                      Reset the RF mode of operation for this radio to
                               default (2.4GHz on radio1, 5GHz on radio2,
                               sensor on radio3)
  rifs                         Configure Reduced Interframe Spacing (RIFS)
                               parameters
  rts-threshold                Reset the RTS threshold to its default (65536)
  shutdown                     Re-enable the selected interface
  smart-rf                     Reset smart-rf related configuration to default
  sniffer-redirect             Disable capture and redirection of packets
  stbc                         Configure Space-Time Block Coding (STBC)
                               parameters
  transmit-beamforming         Disable Transmit Beamforming
  use                          Set setting to use
  wips                         Wireless intrusion prevention related
                               configuration
  wireless-client              Configure wireless client related parameters
  wlan                         Disable a wlan from this radio

  service                      Service Commands

rfs6000-37FABE(config-profile-ap71xxTest-if-radio1)#
```

The following example shows radio interface settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  description "Primary radio to use"
  channel 1
  data-rates b-only
  mesh client
  beacon period 50
  beacon dtim-period bss 1 5
  beacon dtim-period bss 2 2
  beacon dtim-period bss 3 5
  beacon dtim-period bss 4 5
  beacon dtim-period bss 5 5
  beacon dtim-period bss 6 5
  beacon dtim-period bss 7 5
  beacon dtim-period bss 8 5
  beacon dtim-period bss 9 5
  beacon dtim-period bss 10 5
  beacon dtim-period bss 11 5
  beacon dtim-period bss 12 5
  beacon dtim-period bss 13 5
  beacon dtim-period bss 14 5
  beacon dtim-period bss 15 5
  beacon dtim-period bss 16 5
  antenna-gain 12.0
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
```

```
  antenna-mode 2x2
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#no channel
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#no antenna-gain
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#no description
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#no antenna-mode
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#no beacon dtim-period
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#no beacon period
```

The following example shows radio interface settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  mesh client
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

7.1.36.5.30 non-unicast

interface-config-radio-instance

Configures support for forwarding of non-unicast (multicast and broadcast) frames on this radio

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
non-unicast [forwarding|queue|tx-rate]

non-unicast forwarding [follow-dtim|power-save-aware]

non-unicast queue [<1-200>|bss]
non-unicast queue [<1-200>|bss <1-16> <1-200>]

non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]
non-unicast tx-rate bss <1-16> [dynamic-all|dynamic-basic|highest-basic|lowest-basic]
```

Parameters

- `non-unicast forwarding [follow-dtim|power-save-aware]`

non-unicast forwarding	Enables non-unicast frame forwarding on this radio. Once enabled, select one of the available options to specify whether these frames should always *follow DTIM*, or only follow DTIM when using *power save aware* mode.
follow-dtim	Specifies frames always wait for the DTIM interval to time out. The DTIM interval is configured using the *beacon* command. This is the default setting.
power-save-aware	Enables immediate forwarding of frames only if all associated wireless clients are in the power save mode

- `non-unicast queue [<1-200>|bss <1-16> <1-200>]`

non-unicast queue	Enables non-unicast frame forwarding on this radio. Once enabled, specify the number of broadcast packets queued per BSS on this radio. This option is enabled by default. This command also enables you to override the default on a specific BSS.
<1-200>	Specify a number from 1 - 200. This value applies to all BSSs. The default is 50 frames per BSS.
bss <1-16> <1-200>	Overrides the default on a specified BSS • <1-16> – Select the BSS number from 1 - 16. • <1-200> – Specify the number of broadcast packets queued for the selected BSS from 1 - 200.

- `non-unicast tx-rate [bss <1-16>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]`

non-unicast tx-rate	Enables non-unicast frame forwarding on this radio. Once enabled, use one of the available options to configure the rate at which these frames are transmitted.
bss <1-16>	Overrides the default on a specified BSS • <1-16> – Select the BSS number from 1 - 16. The transmit rate selected is applied only to the BSS specified here. The tx-rate options are: dynamic-all, dynamic-basic, highest-basic, lowest-basic.

dynamic-all	Dynamically selects a rate from all supported rates based on current traffic conditions
dynamic-basic	Dynamically selects a rate from all supported basic rates based on current traffic conditions
highest-basic	Uses the highest configured basic rate. This is the default setting.
lowest-basic	Uses the lowest configured basic rate

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#non-unicast queue bss 2
3

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#non-unicast tx-rate bss
1 dynamic-all

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  mesh client
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
  non-unicast tx-rate bss 14 highest-basic
  non-unicast tx-rate bss 15 highest-basic
  non-unicast tx-rate bss 16 highest-basic
  non-unicast queue bss 1 50
  non-unicast queue bss 2 3
--More--
  antenna-diversity
  max-clients 100
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the handling of non-unicast frames to its default

7.1.36.5.31 off-channel-scan

interface-config-radio-instance

Enables off channel scanning on this radio. This option is disabled by default.

Channel scanning uses the access point's resources and is time consuming. Therefore, enable this option only if the radio has the bandwidth to support channel scan without negatively impacting client support.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
off-channel-scan {channel-list|max-multicast|scan-interval|sniffer-redirect}

off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}

off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}

off-channel-scan {sniffer-redirect tzsp <IP>}
```

Parameters

- `off-channel-scan {channel-list [2.4Ghz|5Ghz]} {<CHANNEL-LIST>}`

off-channel-scan	Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.
channel-list [2.4GHz|5GHz]	Optional. Selects the 2.4GHz or 5GHz access point radio band. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all channels. • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<CHANNEL-LIST>	Optional. Specifies a list of 20 MHz, 40 MHz, or 80 MHz channels for the selected band (the channels are separated by commas or hyphens)

- `off-channel-scan {max-multicast <0-100>|scan-interval <2-100>}`

off-channel-scan	Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.
max-multicast <0-100>	Optional. Configures the maximum multicast/broadcast messages used to perform OCS • <0-100> – Specify a value from 0 - 100. The default is 4.
scan-interval <2-100>	Optional. Configures the scan interval in dtims • <2-100> – Specify a value from 2 - 100. The default is 20 dtims.

- `off-channel-scan {sniffer-redirect tzsp <IP>}`

off-channel-scan	Enables off-channel scanning and configures related parameters. These parameters are optional, and the system configures default settings if no values are specified.
sniffer-redirect tzsp <IP>	Optional. Captures and redirects packets to a host running a packet capture/ analysis tool. Use this command to configure the IP address of the host. • tzsp – Encapsulates captured packets in TZSP before redirecting to the specified host • <IP> – Specify the destination device IP address.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#off-channel-scan
channel-list 2.4GHz 1

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
  non-unicast tx-rate bss 14 highest-basic
  non-unicast tx-rate bss 15 highest-basic
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables radio off channel scanning

7.1.36.5.32 placement

interface-config-radio-instance

Defines the radio's location (whether the radio is deployed indoors or outdoors). The radio's placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
placement [indoor|outdoor]
```

Parameters

- `placement [indoor|outdoor]`

placement	Defines the radio's location
indoor	Radio is deployed indoors (uses indoor regulatory rules). This is the default setting.
outdoor	Radio is deployed outdoors (uses outdoor regulatory rules)

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#placement outdoor

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
  non-unicast tx-rate bss 13 highest-basic
  non-unicast tx-rate bss 14 highest-basic
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets a radio's deployment location

7.1.36.5.33 power

interface-config-radio-instance

Configures the radio's transmit power setting

The *transmit power control* (TPC) mechanism automatically reduces the used transmission output power when other networks are within range. Reduced power results in reduced interference issues and increased battery capacity.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
power [<1-30>|smart]
```

Parameters

- `power [<1-30>|smart]`

power	Configures a radio's transmit power
<1-30>	Configures the transmit power from 1 - 30 dBm (actual power could be lower based on regulatory restrictions) For APs with dual or three radios, each radio should be configured with a unique transmit power in respect to its intended client support function.
smart	Enables Smart RF to determine the optimum transmit power needed. By default APs use Smart RF to determine transmit power.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#power 12

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  power 12
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic

--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets a radio's transmit power

7.1.36.5.34 preamble-short

interface-config-radio-instance

Enables short preamble on this radio. If using an 802.11bg radio, enable short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533

Syntax

```
preamble-short
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#preamble-short

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  power 12
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
  non-unicast tx-rate bss 7 highest-basic
  non-unicast tx-rate bss 8 highest-basic
  non-unicast tx-rate bss 9 highest-basic
  non-unicast tx-rate bss 10 highest-basic
  non-unicast tx-rate bss 11 highest-basic
  non-unicast tx-rate bss 12 highest-basic
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables the use of short preamble on a radio

7.1.36.5.35 probe-response

interface-config-radio-instance

Configures transmission parameters for probe response frames

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
probe-response [rate|retry|rssi-threshold]

probe-response retry
probe-response rate [follow-probe-request|highest-basic|lowest-basic]
probe-response rssi-threshold <-128--40>
```

Parameters

- `probe-response retry`

probe-response retry	Enables retransmission of probe-response frames if no acknowledgement is received from the client. This option is enabled by default.

- `probe-response rate [follow-probe-request|highest-basic|lowest-basic]`

probe-response rate	Configures the rates used for transmission of probe response frames. The tx-rate options available for transmitting probe response frames are: follow-probe-request, highest-basic, lowest-basic.
follow-probe-request	Transmits probe responses at the same rate as the received request (default setting)
highest-basic	Uses the highest configured basic rate
lowest-basic	Uses the lowest configured basic rate

- `probe-response rssi-threshold <-128--40>`

probe-response rssi-threshold <-128--40>	Ignores probe request from client if the received signal strength is less than the RSSI threshold specified here <-128--40> – Specify a value from -128 - -40.

Example

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#probe-response rate highest-
basic

nx9500-6C8809(config-profile-testAP7161-if-radio1)#probe-response retry

nx9500-6C8809(config-profile-testAP7161-if-radio1)#probe-response rssi-threshold
-60

nx9500-6C8809(config-profile-testAP7161-if-radio1)#show context
 interface radio1
  probe-response rate highest-basic
  probe-response rssi-threshold -60
nx9500-6C8809(config-profile-testAP7161-if-radio1)#
```

Related Commands

no	Resets transmission parameters for probe response frames

7.1.36.5.36 radio-resource-measurement

interface-config-radio-instance

Enables 802.11k radio resource measurement. When enabled, the radio station sends channel and neighbor reports.

The IEEE 802.11 Task Group k defined a set of specifications regarding radio resource measurements. These specifications specify the radio resources to be measured and the mechanism used to communicate measurement requests and results.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]
```

Parameters

- `radio-resource-measurement [attenuation-threshold <1-199>|max-entries <1-12>]`

radio-resource-measurement	Enables 802.11k radio resource measurement on the radio
attenuation-threshold <1-199>	Configures the neighbor attenuation threshold, considered when generating channel and neighbor reports • <1-199> – Specify the attenuation threshold from 1 -199. The default is 90.
max-entries <1-12>	Configures the maximum number of entries to include in channel and neighbor reports • <1-12> – Specify a value from 1 - 12. The default is 6.

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radio1)#radio-resource-
measurement attenuation-threshold 20

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radio1)#radio-resource-
measurement max-entries 10

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radio1)#show context
 interface radio1
  radio-resource-measurement max-entries 10
  radio-resource-measurement attenuation-threshold 20
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-radio1)#
```

Related Commands

no	Disables 802.11k radio resource measurement support

7.1.36.5.37 radio-share-mode

interface-config-radio-instance

Configures the radio's mode of operation as radio share. A radio operating in the radio share mode services clients and also performs sensor functions (defined by the radio's *AirDefense Services Platform* (ADSP) licenses and profiles).

NOTE: The sensor capabilities of the radio are restricted to the channel and WLANs defined on the radio.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533

Syntax

```
radio-share-mode [inline|off|promiscuous]
```

Parameters

- `radio-share-mode [inline|off|promiscuous]`

radio-share-mode	Enables sharing of packets, switched by this radio, with the WIPS sensor module. There are two radio-share modes, these are: inline and promiscuous
inline	Enables sharing of all WLAN packets (matching the BSSID of the radio) serviced by the radio with the WIPS sensor module.
off	Disables radio share (no packets shared with the WIPS sensor module)
promiscuous	Enables the *promiscuous radio share* mode. In this mode the radio is configured to receive all packets on the channel irrespective of whether the destination address is the radio or not, and shares these packets with the WIPS sensor module for analysis (i.e. without filtering based on BSSI).

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#radio-share-mode
promiscuous

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  power 12
  data-rates b-only
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  preamble-short
  guard-interval long
  ..........................................................
  non-unicast queue bss 16 50
  antenna-diversity
  max-clients 100
  radio-share-mode promiscuous
  airtime-fairness prefer-ht weight 6
  lock-rf-mode
  extended-range 15
  antenna-downtilt
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the radio share mode for this radio to its default

7.1.36.5.38 rate-selection

interface-config-radio-instance

Sets the data-rate selection mode to standard or opportunistic

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
rate-selection [opportunistic|standard]
```

Parameters

- `rate-selection [opportunistic|standard]`

rate-selection	Sets the rate selection mode to standard or opportunistic
standard	Configures the monotonic rate selection mode. This is the default setting.
opportunistic	Configures the *opportunistic radio link adaptation* (ORLA) rate selection mode The ORLA algorithm is designed to select data rates that provide best throughput. Instead of using local conditions to decide whether a data rate is acceptable or not, ORLA pro-actively probes other rates to determine if greater throughput is available. If these other rates do provide improved throughput, ORLA intelligently adjusts its selection tables to favour higher performance. ORLA provides improvements both on the client side of a mesh network as well as in the backhaul capabilities. **Note:** The ORLA rate selection mode is supported only on the AP7161 and AP8163 model access points.

Example

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#rate-selection opportunistic

nx9500-6C8809(config-profile-testAP7161-if-radio1)#show context
 interface radio1
  rate-selection opportunistic
nx9500-6C8809(config-profile-testAP7161-if-radio1)#
```

Related Commands

no	Resets the rate selection mode to standard (monotonic)

7.1.36.5.39 rf-mode

interface-config-radio-instance

Configures the radio's RF mode of operation

This command sets the mode to either 2.4 GHz WLAN or 5.0 GHz WLAN support depending on the radio's intended client support. If you are currently licensed to use 4.9 GHz, configure the 4.9 GHz-WLAN option.

Set the mode to sensor if using the radio for rogue device detection. The radio cannot support rogue detection when one of the other radios is functioning as a WIPS sensor. To set a radio as a detector, disable sensor support on the other access point radios.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|bridge|scan-ahead|sensor]
```

Parameters

- `rf-mode [2.4GHz-wlan|4.9GHz-wlan|5GHz-wlan|bridge|scan-ahead|sensor]`

rf-mode	Configures the radio's RF mode of operation
2.4GHz-wlan	Provides WLAN service in the 2.4 GHz bandwidth
4.9GHz-wlan	Provides WLAN service in the 4.9 GHz bandwidth
5GHz-wlan	Provides WLAN service in the 5.0 GHz bandwidth
bridge	Enables this radio to operate as client bridge that can authenticate and associate to a defined infrastructure *Wireless LAN* (WLAN) access point **Note:** This option is applicable only on the AP6522, AP6562, AP7522, AP7532, and AP7562 model access points. Enable this option only if the access point is to provide client-bridge support. Once enabled, configure the client-bridge parameters. For more information, see *bridge*.
scan-ahead	Enables this radio to operate as a scan-ahead radio A radio functioning in the scan-ahead mode is used for forward scanning only. The radio does not support WLAN or mesh services. The scan ahead feature is used in *Dynamic Frequency Selection* (DFS) aware countries for infrastructure devices, static, and *vehicular mounted modems* (VMMs). It enables a secondary radio to scan ahead for an active channel for backhaul transmission, in the event of a radar trigger on the primary radio. The device then switches radios allowing transmission to continue. This is required in environments where handoff is required and DFS triggers are common. With a secondary radio dedicated for forward scanning, the primary radio, in case of radar hit, hands over the *channel availability check* (CAC) function to the secondary radio. This avoids a break in data communication, which would have resulted if the primary radio was to do CAC itself. The secondary radio periodically does a scan of the configured channel list, searching for the other available meshpoint roots. When configured on the root meshpoint, the scan-ahead feature also scans for cleaner channels.

sensor	Operates as a sensor radio. Configures this radio to function as a scanner, providing scanning services on both 2.4 GHz and 5.0 GHz bands. The radio does not provide WLAN services.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#rf-mode sensor

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the radio's RF mode of operation
data-rates	Configures the 802.11 data rates on this radio

7.1.36.5.40 rifs

interface-config-radio-instance

Configures *Reduced Interframe Spacing* (RIFS) parameters on this radio

This value determines whether interframe spacing is applied to access point transmitted or received packets, both, or none. Inter-frame spacing is the interval between two consecutive Ethernet frames that enable a brief recovery between packets and allow target devices to prepare for the reception of the next packet.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
rifs [none|rx-only|tx-only|tx-rx]
```

Parameters

- `rifs [none|rx-only|tx-only|tx-rx]`

rifs	Configures RIFS parameters
none	Disables support for RIFS Consider setting the value to None for high-priority traffic to reduce packet delay.
rx-only	Supports RIFS possession only
tx-only	Supports RIFS transmission only
tx-rx	Supports both RIFS transmission and possession (default setting)

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#rifs tx-only

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables radio's RIFS parameters

7.1.36.5.41 rts-threshold

interface-config-radio-instance

Configures the *Request to Send* (RTS) threshold value on this radio

RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path.

The RTS threshold controls RTS/CTS by initiating an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.

Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's access point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.

A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
rts-threshold <0-65536>
```

Parameters

- `rts-threshold <0-65536>`

rts-threshold <0-65536>	Specify the RTS threshold value from 0 - 65536 bytes. The default is 65536 bytes.

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#rts-threshold 100

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only

--More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets a radio's RTS threshold to its default

7.1.36.5.42 service

interface-config-radio-instance

Enables dynamic control function. This dynamic function controls performance of the radio receiver's *low noise amplifiers* (LNAs).

When enabled, the control function, in the presence of very strong received signals, improves the receiver's performance on radio 1. Strong signals are caused if the distance between the WiFi client and the AP is within two (2) meters. When disabled, the control function is a useful debug tool in case the uplink throughput is less than expected and the AP-to-client separation is greater than two (2) meters. Disabling the control function does not affect the receive sensitivity of the radio.

Supported in the following platforms:

- Access Points — AP6522, AP6562

Syntax

```
service radio-lna [agc|ms]
```

Parameters

- `service radio-lna [agc|ms]`

service radio-lna [agc|ms]	Enables dynamic control function • agc – Enables dynamic LNA control function. This is the default setting. • ms – Disables dynamic LNA control function

Example

```
nx9500-6C8809(config-profile-testAP6522-if-radio1)#service radio-lna ms

nx9500-6C8809(config-profile-testAP6522-if-radio1)#show context
 interface radio1
  service radio-lna ms
nx9500-6C8809(config-profile-testAP6522-if-radio1)#
```

Related Commands

no	Reverts radio-lna mode to default (agc)

7.1.36.5.43 shutdown

interface-config-radio-instance

Terminates or shuts down selected radio interface

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#shutdown
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Enables a disabled radio interface

7.1.36.5.44 smart-rf

interface-config-radio-instance

Overrides Smart RF channel width setting on this radio. When configured, the radio overrides the Smart RF selected channel setting and operates in the channel configured using this command.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
smart-rf preferred-channel-width [20MHz|40MHz|80MHz]
```

Parameters

- `smart-rf preferred-channel-width [20MHz|40MHz|80MHz]`

smart-rf preferred-channel-width [20MHz|40MHz|80MHz]	Configures the preferred channel width. The options are: • 20MHz – Sets 20 MHz as the preferred channel of operation • 40MHz – Sets 40MHz as the preferred channel of operation • 80MHz – Sets 80MHz as the preferred channel of operation (default setting)

Example

```
nx9500-6C8809(config-profile-testAP7161-if-radio1)#smart-rf preferred-channel-
width 40MHz

nx9500-6C8809(config-profile-testAP7161-if-radio1)#show context
 interface radio1
  smart-rf preferred-channel-width 40MHz
  rate-selection opportunistic
nx9500-6C8809(config-profile-testAP7161-if-radio1)#
```

Related Commands

no	Enables use of Smart RF selected channel of operation

7.1.36.5.45 sniffer-redirect

interface-config-radio-instance

Captures and redirects packets to an IP address running a packet capture/analysis tool

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
sniffer-redirect [omnipeek|tzsp] <IP> channel [1|10|100|100w --------] {snap <1-65535> (append descriptor)}
```

Parameters

```
• sniffer-redirect [omnipeek|tzsp] <IP> channel [1|10|100|100w ---------] {snap <1-65535> (append descriptor)}
```

sniffer-redirect	Captures and redirects packets to an IP address running a packet capture/analysis tool
omnipeek	Encapsulates captured packets in proprietary header (used with OmniPeek and plug-in)
tzsp	Encapsulates captured packets in TZSP (used with WireShark and other tools)
<IP>	Specify the IP address of the device running the capture/analysis tool (the host to which captured off channel scan packets are redirected)
[1|10|100|100w ---------]	Specify the channel to capture packets • 1 – Channel 1 in 20 MHz mode (default setting) • 10 – Channel 10 in 20 MHz mode • 100 – Channel 100 in 20 MHz mode • 100w – Channels 100w in 40 MHz mode (channels 100*,104)
snap <1-65535>	Optional. Allows truncating of large captured frames at a specified length (in bytes). This option is useful when capturing traffic with large frames. Use this option when only headers are needed for analysis, since it reduces the bandwidth needed for sniffing, and (for typical values) eliminates any fragmentation of the outer packet. • <1-65535> – Specify the maximum truncated byte length of captured packets.
append descriptor	Optional – Enables appending of the radio's receive descriptor to the captured packet

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#sniffer-redirect
omnipeek 172.16.10.1 channel 1

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
```

```
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic
  non-unicast tx-rate bss 3 highest-basic
  non-unicast tx-rate bss 4 highest-basic
  non-unicast tx-rate bss 5 highest-basic
  non-unicast tx-rate bss 6 highest-basic
 --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables packet capture and redirection

7.1.36.5.46 stbc

interface-config-radio-instance

Configures the radio's *Space Time Block Coding* (STBC) mode. STBC is a pre-transmission encoding scheme providing an improved SNR ratio (even at a single RF receiver). STBC transmits multiple data stream copies across multiple antennas. The receiver combines the copies into one to retrieve data from the signal. These transmitted data versions provide redundancy to increase the odds of receiving data streams with a good data decode (especially in noisy environments).

NOTE: STBC requires the radio has at least two antennas with the capability to transmit two streams. If the antenna mode is configured to 1x1 (or falls back to 1x1 for some reason), STBC support is automatically disabled.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
stbc [auto|none|tx-only]
```

Parameters

- `stbc [auto|none|tx-only]`

stbc	Configures the radio's STBC mode
auto	Autoselects STBC settings based on the platform type and other radio interface settings. This is the default setting.
none	Disables STBC support
tx-only	Configures the AP radio to format and broadcast the special stream (enables STBC support for transmit only)

Example

```
rfs6000-37FABE(config-profile-81xxTestProfile-if-radio1)#stbc tx-only

rfs6000-37FABE(config-profile-81xxTestProfile-if-radio1)#show context
 interface radio1
  stbc tx-only
rfs6000-37FABE(config-profile-81xxTestProfile-if-radio1)#
```

Related Commands

no	Disables STBC support

7.1.36.5.47 transmit-beamforming

interface-config-radio-instance

Enables transmit beamforming on this radio interface. This option is disabled by default.

When enabled, this option steers signals to peers in a specific direction to enhance signal strength and improve throughput amongst meshed devices (not clients). Each access point radio supports up to 16 beamforming capable mesh peers. When enabled, a beamformer steers its wireless signals to its peers. A beamformee device assists the beamformer with channel estimation by providing a feedback matrix. The feedback matrix is a set of values sent by the beamformee to assist the beamformer in computing a steering matrix. A steering matrix is an additional set of values used to steer wireless signals at the beamformer so constructive signals arrive at the beamformee for better SNR and throughput. Any beamforming capable mesh peer connecting to a radio whose capacity is exhausted cannot enable beamforming itself.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562,AP8122, AP8132, AP8163, AP8432, AP8533

Syntax

```
transmit-beamforming
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-testAP81XX-if-radio1)#transmit-beamforming
```

Related Commands

no	Disables transmit beamforming on this radio interface

7.1.36.5.48 use

interface-config-radio-instance

Applies an association ACL policy and a radio QoS policy on this radio interface

An association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a controller managed access point radio. An ACL is a sequential collection of permit and deny conditions that apply to controller packets. When a packet is received on an interface, the controller compares the fields in the packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
use [association-acl-policy|radio-qos-policy]

use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy <RADIO-QOS-POLICY-NAME>]
```

Parameters

```
• use [association-acl-policy <ASSOC-ACL-POLICY-NAME>|radio-qos-policy <RADIO-QOS-POLICY-NAME>]
```

use	Applies an association ACL policy and a radio QoS policy on this radio interface
association-acl-policy	Uses a specified association ACL policy with this radio interface • <ASSOC-ACL-POLICY-NAME> – Specify the association ACL policy name (should be existing and fully configured).
radio-qos-policy	Uses a specified radio QoS policy with this radio interface • <RADIO-QoS-POLICY-NAME> – Specify the radio QoS policy name (should be existing and fully configured).

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#use association-acl-policy test

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  use association-acl-policy test
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Dissociates the specified association ACL policy and radio QoS policy

7.1.36.5.49 wips

interface-config-radio-instance

Enables access point to change its channel of operation in order to terminate rogue devices. The radio should be configured to provide WLAN service.

This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

NOTE: AP7522 and AP7532 access points use Smart RF to perform off-channel scans. Therefore, ensure that a Smart RF policy is configured and applied to AP7522 and AP7532 access points RF Domains to enable them perform rogue detection and termination.

Syntax

```
wips airtime-termination allow-channel-change
```

Parameters

- `wips airtime-termination allow-channel-change`

wips airtime-termination allow-channel-change	Enables access point to change its channel of operation (to that of the rogue device) in order to terminate the rogue device

Example

```
nx9500-6C8809(config-profile-testAP81XX-if-radio1)#wips air-termination allow-channel-change
```

Related Commands

no	Disables access point to change its channel of operation in order to terminate rogue devices

7.1.36.5.50 wireless-client

interface-config-radio-instance

Configures wireless client parameters on this radio

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
wireless-client tx-power [<0-20>|mode]

wireless-client <0-20>

wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]
```

Parameters

- `wireless-client tx-power <0-20>`

wireless-client	Configures wireless client parameters
tx-power <0-20>	Configures the transmit power indicated to wireless clients. If using a dual or three radio model access point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value. • <0-20> – Specify transmit power from 0 - 20 dBm.

- `wireless-client tx-power mode [802.11d {wing-ie}|wing-ie {802.11d}]`

wireless-client	Configures wireless client parameters

tx-power [802.11d|wing-ie]	Configures the transmit power indicated to wireless clients
	• 802.11d – Advertises in the IEEE 802.11d country information element
	  • wing-ie – Optional. Advertises in the WiNG information element (173)
	• wing-ie – Advertises in the WiNG information element (173). This is the default setting.
	  • 802.11d – Optional. Advertises in the IEEE 802.11d country information element

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#wireless-client tx-power
20

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  wireless-client tx-power 20
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
   --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Resets the transmit power indicated to wireless clients

7.1.36.5.51 wlan

interface-config-radio-instance

Enables a WLAN on this radio

Use this command to configure WLAN/BSS mappings for an existing access point deployment. Administrators can assign each WLAN its own BSSID. If using a single-radio access point, there are 8 BSSIDs available. If using a dual-radio access point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
wlan <WLAN-NAME> {bss|primary}

wlan <WLAN-NAME> {bss <1-16>} {primary}
```

Parameters

- `wlan <WLAN-NAME> {bss <1-16>} {primary}`

<WLAN-NAME> {bss <1-16> |primary}	Specify the WLAN name (it must have been already created and configured)
	• bss <1-16> – Optional. Specifies a BSS for the radio to map the WLAN
	  • <1-18> – Specify the BSS number from 1 - 16.
	  • primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS
	• primary – Optional. Uses the specified WLAN as the primary WLAN, when multiple WLANs exist on the BSS

Example

```
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#wlan TestWLAN primary

rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#show context
 interface radio1
  rf-mode sensor
  placement outdoor
  mesh client
  rts-threshold 100
  wireless-client tx-power 20
  wlan TestWLAN bss 1 primary
  off-channel-scan channel-list 2.4GHz 1
  guard-interval long
  aggregation ampdu tx-only
  rifs tx-only
  use association-acl-policy test
  sniffer-redirect omnipeek 172.16.10.1 channel 1
  aeroscout forward
  ekahau forward ip 172.16.10.1 port 3
  non-unicast tx-rate bss 1 dynamic-all
  non-unicast tx-rate bss 2 highest-basic

  --More--
rfs6000-37FABE(config-profile-71xxTestProfile-if-radio1)#
```

Related Commands

no	Disables a WLAN on a radio

7.1.36.6 interface-config-wwan-instance

interface

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a device to connect, transmit and receive data over a Cellular Wide Area Network. The RFS4000 and RFS6000 each have a PCI Express card slot that supports 3G WWAN cards. The WWAN card uses *point to point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP is the protocol used for establishing Internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

To switch to the WWAN Interface configuration mode, use the following command:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <DEVICE-PROFILE-NAME>

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#interface wwan1

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#?
Interface configuration commands:
  apn           Enter the access point name provided by the service provider
  auth-type     Type of authentication, Eg chap, pap
  crypto        Encryption Module
  description   Port description
  ip            Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Enter password provided by the service provider
  shutdown      Disable wireless wan feature
  use           Set setting to use
  username      Enter username provided by the service provider

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#
```

The following table summarizes WWAN interface configuration commands:

Commands	Description	Reference
apn	Configures the access point's name provided by the service provider	*page 7-328*
auth-type	Configures the authentication types used on this interface	*page 7-329*
crypto	Associates a crypto map with this interface	*page 7-330*
ip	Associates an IP ACL with this interface	*page 7-331*
no	Removes or reverts the WWAN interface settings	*page 7-332*
password	Configures a password for this WWAN interface	*page 7-333*
use	Associates an IP ACL with this interface	*page 7-335*
username	Configures the names of users accessing this interface	*page 7-336*

7.1.36.6.1 apn

interface-config-wwan-instance

Configures the cellular data provider's name. This setting is needed in areas with multiple cellular data providers using the same protocols, such as Europe and Asia.

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
apn <WORD>
```

Parameters

- `apn <WORD>`

apn <WORD>	Specify the name of the cellular data service provider.

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#apn AT&T

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  apn AT&T
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes the configured access point name.

7.1.36.6.2 auth-type

interface-config-wwan-instance

Configures the authentication type used by the cellular data provider

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
auth-type [chap|mschap|mschap-v2|pap]
```

Parameters

- `auth-type [chap|mschap|mschap-v2|pap]`

auth-type	Configures the authentication protocol used on this interface. The options are: PAP, CHAP, MSCHAP, and MSCHAP-v2
chap	Configures *Challenge-Handshake Authentication Protocol* (CHAP). This is the default value.
mschap	Configures *Microsoft Challenge-Handshake Authentication Protocol* (MSCHAP)
mschapv2	Configures *Microsoft Challenge-Handshake Authentication Protocol* (MSCHAP) version 2
pap	Configures *Password Authentication Protocol* (PAP)

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#auth-type mschap-v2

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  apn AT&T
  auth-type mschap-v2
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes the authentication protocol configured on this interface

7.1.36.6.3 crypto

interface-config-wwan-instance

Associates a crypto map with this interface

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
crypto map <CRYPTO-MAP-NAME>
```

Parameters

- `crypto map <CRYPTO-MAP-NAME>`

crypto map <CRYPTO-MAP-NAME>	Associates a crypto map with this interface • <CRYPTO-MAP-NAME> – Specify the crypto map name (should be existing and configured).

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#crypto map test

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  apn AT&T
  auth-type mschap-v2
  crypto map test
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes the crypto map associated with this interface

7.1.36.6.4 ip

interface-config-wwan-instance

Configures IP related settings on this interface

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
ip [default-gateway|nat]

ip default-gateway priority <1-8000>

ip nat [inside|outside]
```

Parameters

- `ip default-gateway priority <1-8000>`

ip	Configures IP related settings on this interface
default-gateway priority <1-8000>	Configures the default-gateway's (learned by the wireless WAN) priority. • <1-8000> – Specify a value from 1 - 8000. The default is 3000.

- `ip nat [inside|outside]`

ip	Configures IP related settings on this interface
nat [inside|outside]	Configures the NAT settings. This option is disabled by default. • inside – Marks this WWAN interface as NAT inside. The inside network is transmitting data over the network to its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. • outside – Marks this WWAN interface as NAT outside. Packets passing through the NAT on the way back to the controller or service platform managed LAN are matched against the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#ip default-gateway priority 1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#ip nat inside

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  apn AT&T
  auth-type mschap-v2
  crypto map test
  ip nat inside
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes IP related settings on this interface

7.1.36.6.5 no

interface-config-wwan-instance

Removes or reverts the WWAN interface settings

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
no [all|apn|auth-type|crypto|description|ip|password|shutdown|use|username]

no [all|apn|auth-type|description|password|shutdown|username]

no crypto map

no ip [default-gateway priority|nat]

no use ip-access-list in
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts this WWAN interface's settings based on the parameters passed

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example displays the WWAN interface settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  apn AT&T
  auth-type mschap-v2
  crypto map test
  ip nat inside
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#no apn
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#no auth-type
```

The following example displays the WWAN interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  crypto map test
  ip nat inside
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

7.1.36.6.6 password

interface-config-wwan-instance

Configures a password for this WWAN interface. The configured value is used for authentication support by the cellular data carrier.

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
password [2 <WORD>|<WORD>]
```

Parameters

- `password [2 <WORD>|<WORD>]`

password	Configures a password for this WWAN interface
2 <WORD>	Configures an encrypted password. Use this option when copy pasting the password from another device.
<WORD>	Enter the password string (should not exceed 32 characters in length.

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#password 2 TechPubsTesting@123

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes the configured password

7.1.36.6.7 shutdown

interface-config-wwan-instance

Shuts down this WWAN interface. Use the no > shutdown command to re-start the WWAN interface.

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
shutdown
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#shutdown

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  shutdown
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Re-starts the WWAN interface

7.1.36.6.8 use

interface-config-wwan-instance

Associates an IP ACL with this interface. The ACL should be existing and configured.

The ACL applies an IP based firewall to all incoming packets. The ACL identifies a single IP or a range of IPs that are to be allowed or denied access on this interface.

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
use ip-access-list in <ACCESS-LIST-NAME>
```

Parameters

- `use ip-access-list in <ACCESS-LIST-NAME>`

use ip-access-list in <ACCESS-LIST-NAME>	Associates an inbound IPv4 ACL with this interface. This setting applies to IPv4 inbound traffic only and not IPv6 traffic. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike TCP). IPv4 hosts can use link local addressing to provide local connectivity. • <ACCESS-LIST-NAME> – Specify the IP ACL name.

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#use ip-access-list in test

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  use ip-access-list in test
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes the IP ACL associated with this interface

7.1.36.6.9 username

interface-config-wwan-instance

Configures the names of users accessing this interface

Supported in the following platforms:

- Access Point — AP7161, AP81XX, AP8232
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
username <WORD>
```

Parameters

- `username <WORD>`

username <WORD>	Configures the username for authentication support by the cellular data carrier • <WORD> – Specify the username (should not exceed 32 characters).

Example

```
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#username TechPubsUser1

nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#show context
 interface wwan1
  username TechPubsUser1
  password TechPubsTesting@123
  crypto map test
  ip nat inside
  use ip-access-list in test
  ip default-gateway priority 1
nx9500-6C8809(config-profile-testRFS6000-if-wwan1)#
```

Related Commands

no	Removes the configured username

7.1.36.7 interface-config-bluetooth-instance

interface

AP8432 and AP8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP8432 and AP8533 models support both Bluetooth classic and *Bluetooth low energy* (BLE) technology. These platforms use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

NOTE: AP8132 model access points support an external USB Bluetooth radio providing ADSP Bluetooth classic sensing functionality only, not the BLE beaconing functionality available for AP8432 and AP8533 model access points described in this section.

AP8432 and AP8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets periodically. These advertisement packets are short and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are customizable via the Bluetooth radio interface configuration context.

To switch to this mode, use the following commands:

```
<DEVICE>(config)#profile <ap8432/ap8533> <PROFILE-NAME>

<DEVICE>(config-profile-default-ap8432)#interface bluetooth ?
  <1-1>  Bluetooth interface index?
```

The following example uses the default-ap8432 profile instance to configure the Bluetooth radio interface:

```
nx9500-6C8809(config-profile-default-ap8432)#interface bluetooth 1
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
Bluetooth Radio Mode commands:
  beacon       Configure low-energy beacon operation parameters
  description  Configure a description for this bluetooth radio
  eddystone    Configure eddystone beacon payload parameters
  ibeacon      Configure iBeacon beacon payload parameters
  mode         Set the bluetooth opreation mode
  no           Negate a command or set its defaults
  shutdown     Shutdown the selected bluetooth radio interface

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Commands	Description	Reference
beacon	Configures the Bluetooth radio's beacon's emitted transmission pattern	*page 7-339*
description	Configures a description for the Bluetooth radio interface	*page 7-341*

Commands	Description	Reference
eddystone	Configures Eddystone beacon payload parameters. Configure these parameters if the operational mode is set to 'le-beacon' and the beacon transmission pattern is set to 'eddystone-url1' or 'eddystone-url2'.	*page 7-342*
ibeacon	Configures iBeacon beacon payload parameters. Configure these parameters if the operational mode is set to 'le-beacon' and the beacon transmission pattern is set to 'ibeacon'.	*page 7-343*
mode	Configures the Bluetooth radio's mode of operation	*page 7-345*
shutdown	Shutdowns the selected Bluetooth radio interface	*page 7-346*
no	Removes or reverts to default this Bluetooth radio interface's settings	*page 7-347*

7.1.36.7.1 beacon

interface-config-bluetooth-instance

Configures the Bluetooth radio's beacon's emitted transmission pattern for Bluetooth radios functioning in the *low energy beacon* (le-beacon) mode. This option is applicable *only if* the Bluetooth radio's operational mode is set to *le-beacon*.

Supported in the following platforms:

- Access Points – AP8432, AP8533

Syntax

```
beacon [pattern|period]

beacon pattern [eddystone-url1|eddystone-ulr2|ibeacon]

beacon period <100-10000>
```

Parameters

- `beacon pattern [eddystone-url1|eddystone-ulr2|ibeacon]`

beacon pattern [eddystone-url1| eddystone-ulr2| ibeacon]	When the beacon mode is set to 'le-beacon', use this command to configure the Bluetooth radio's beacon's emitted transmission pattern. Select one of the following beacon patterns: • eddystone-url1 – Transmits an Eddystone-URL beacon using URL 1. This is the default setting. • eddystone-url2 – Transmits an Eddystone-URL beacon using URL 2 An Eddystone-URL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for Internet access. If an Eddystone-URL beacon broadcasts https:anysite, clients receiving the packet can access that URL. If setting the transmission pattern as 'eddystone-url1' or 'eddystone-ulr2', use the 'eddystone' keyword to configure Eddystone beacon payload parameters. For more information, see *eddystone*. • ibeacon – Transmits an ibeacon beacon. iBeacon was created by Apple for use in *iPhone OS* (iOS) devices (beginning with iOS version 7.0). There are three data fields Apple has made available to iOS applications, a *Universally Unique IDentifier* (UUID) for device identification, a *Major* value for device class and a *Minor* value for more refined information like product category. If setting the transmission pattern as 'ibeacon', use the 'ibeacon' keyword to configure ibeacon beacon payload parameters. For more information, see *ibeacon*. For more information on configuring the Bluetooth radio's operational mode, see *mode*.

- `beacon period <100-10000>`

beacon period <100-10000>	Configures the Bluetooth radio's beacon transmission period, in milliseconds, from 100 - 10000. As the defined period increases, so does the CPU processing time and the number of packets incrementally transmitted (typically one per minute). • <100-10000> – Specify a value from 100 - 10000 milliseconds. The default value is 1000 milliseconds.

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#beacon pattern
eddystone-url2

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#beacon period 900

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  description AP8432-BLE-Radio1
  mode le-beacon
  beacon pattern eddystone-url2
  beacon period 900
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no	Removes or reverts to default this Bluetooth radio's beacon-related configurations

7.1.36.7.2 description

interface-config-bluetooth-instance

Configures a description for the Bluetooth radio interface, differentiating it from other Bluetooth supported radio's within the same RF Domain

Supported in the following platforms:

- Access Points – AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
description <WORD>
```

Parameters

- `description <WORD>`

description <WORD>	Configures a description for the AP8432/AP8533 access point's Bluetooth radio's description • <WORD> – Provide a description that uniquely identifies this radio interface from other similar Bluetooth supported radios (should not exceed 64 characters) within an RF Domain.

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#description AP8432-
BLE-Radio1

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  description AP8432-BLE-Radio1
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no	Removes this Bluetooth radio interface's description

7.1.36.7.3 eddystone

interface-config-bluetooth-instance

Configures Eddystone beacon payload parameters. Configure these parameters only if the Bluetooth radio interface's operational mode is set to 'le-beacon', and the beacon's emitted transmission pattern is set to either 'eddystone-url1' or 'eddystone-ulr2'.

Supported in the following platforms:

- Access Points – AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
eddystone [calibration-rssi <-127-127>|url [1|2] <WORD>]
```

Parameters

- `eddystone [calibration-rssi|url [1|2] <WORD>]`

eddystone [calibration-rssi <-127-127>| url [1|2] <WORD>]	If the Beacon transmission pattern has been set to either 'eddystone-url1' or 'eddystone-url2', configure the following Eddystone parameters:
	• calibration-rssi – Configures the Eddystone beacon measured calibration signal strength, from -127 to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters.
	  • <-127-127> – Specify a value from -127 - 127 dBm. The default value is -19 dBm.
	• url [1|2] <WORD> – Configures the Eddystone URL as URL1 OR URL2
	  • 1 – Selects the Eddystone URL number 1
	  • 2 – Selects the Eddystone URL number 2
	The following keyword is common to the 'eddystone-url1' and 'eddystone-url2' keywrods:
	  • <WORD> – Enter a 64 character maximum *eddystone-URL1/eddystone-URL2*. The URL must be 18 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a Web server.

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#eddystone calibration-
rssi -120

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  description AP8432-BLE-Radio1
  mode le-beacon
  beacon pattern eddystone-url2
  beacon period 900
  eddystone calibration-rssi -120
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no	Removes or reverts to default this Bluetooth radio's Eddystone beacon payload configurations

7.1.36.7.4 ibeacon

interface-config-bluetooth-instance

Configures iBeacon beacon payload parameters. Configure these parameters only if the Bluetooth radio interface's operational mode is set to 'le-beacon', and the beacon's emitted transmission pattern is set to 'ibeacon'.

Supported in the following platforms:

- Access Points – AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
ibeacon [calibration-rssi <-127-127>|major <0-65535>|minor <0-65535>|uuid <WORD>]

ibeacon [calibration-rssi <-127-127>|uuid <WORD>]

ibeacon [major|minor] <0-65535>
```

Parameters

```
• ibeacon [calibration-rssi <-127-127>|major <0-65535>|minor <0-65535>|uuid
<WORD>]
```

ibeacon	Configures following iBeacon beacon payload parameters: calibration-rssi, major, minor, and uuid
calibration-rssi <-127-127>	Configures the ibeacon measured calibration signal strength, from -127 to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. • <-127-127> – Specify a value from -127 - 127 dBm. The default value is -60 dBm.
major <0-65535>	Configures the iBeacon Major value from 0 - 65535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. • <0-65535> – Specify a value from 0 - 65535. The default value is 1111.
minor <0-65535>	Configures the iBeacon Minor value from 0 - 65535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222. • <0-65535> – Specify a value from 0 - 65535. The default value is 2222.
uuid <WORD>	Configures a 32 hex character maximum UUID. The UUID classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes. For example, f2468da65fa82e841134bc5b71e0893e. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration. • <WORD> – Specify the UUID (should not exceed 32 hexadecimal characters). The default value is 01F101F101F101F101F101F101F101F1.

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon calibration-
rssi -70

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon major 1110

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon minor 2210

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#ibeacon uuid
f2468da65fa82e841134bc5b71e0893e
```

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  mode le-beacon
  beacon pattern ibeacon
  ibeacon calibration-rssi -70
  ibeacon major 1110
  ibeacon minor 2210
  ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no	Removes or reverts to default this Bluetooth radio's iBeacon beacon payload parameters

7.1.36.7.5 mode

interface-config-bluetooth-instance

Configures the Bluetooth radio interface's mode of operation as *bt-sensor* or *le-beacon*

Supported in the following platforms:

- Access Points – AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
mode [bt-sensor|le-beacon|le-tracking]
```

Parameters

- `mode [bt-sensor|le-beacon|le-tracking]`

mode	Configures the Bluetooth radio interface's mode of operation. The options are: • bt-sensor – Select this option to provide Bluetooth support for legacy devices. bt-sensors are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically these connections are not ideally suited for the newer *Bluetooth low energy* (BLE) technology supported devices. This is the default setting. • le-beacon – Select this option to provide Bluetooth support for newer BLE technology supported devices. le-beacons are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. le-beacons are not designed as replacements for classic beacon sensors. If selecting this option, use the *beacon* keyword to configure the Beacon transmission period and Beacon transmission pattern. • le-tracking – Select this option to provide Bluetooth support for BLE asset tracking. When enabled, it uses the AP's Bluetooth radio to detect BLE 'asset tags' within the managed network. This information is reported to a back-end server (NSight server).

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#mode le-beacon

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  mode le-beacon
  beacon pattern ibeacon
  ibeacon calibration-rssi -70
  ibeacon major 1110
  ibeacon minor 2210
  ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no	Reverts this Bluetooth radio's mode of operation to *le-beacon*

7.1.36.7.6 shutdown

interface-config-bluetooth-instance

Shutsdown the selected AP8432/AP8533 Bluetooth radio interface

Supported in the following platforms:

- Access Points – AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
shutdown
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#shutdown

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  mode le-beacon
  beacon pattern ibeacon
  ibeacon calibration-rssi -70
  ibeacon major 1110
  ibeacon minor 2210
  ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

Related Commands

no	Reverses shutdown

7.1.36.7.7 no

interface-config-bluetooth-instance

Removes or reverts to default this AP8432/AP8533 Bluetooth radio interface's settings

Supported in the following platforms:

- Access Points – AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
no [beacon|description|eddystone|ibeacon|mode|shutdown]

no beacon [pattern|period]
no description
no eddystone [calibration-rssi|url [1|2]
no ibeacon [calibration-rssi|major|minor|uuid]
no mode
no shutdown
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts to default this Bluetooth radio interface's settings based on the parameters passed • <PARAMETERS> – Specify the parameters.

Example

The following example shows the AP8432 default profile's Bluetooth radio interface settings:

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  shutdown
  mode le-beacon
  beacon pattern ibeacon
  ibeacon calibration-rssi -70
  ibeacon major 1110
  ibeacon minor 2210
  ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#

nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#no shutdown
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#no ibeacon minor
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#no ibeacon
calibration-rssi
```

The following example shows the AP8432 default profile's Bluetooth radio interface settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#show context
 interface bluetooth1
  no shutdown
  mode le-beacon
  beacon pattern ibeacon
  ibeacon major 1110
  ibeacon uuid f2468da65fa82e841134bc5b71e0893e
nx9500-6C8809(config-profile-default-ap8432-if-bluetooth1)#
```

7.1.37 ip

Profile Config Commands

The following table summarizes NAT pool configuration commands:

Command	Description	Reference
ip	Configures IP components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards, etc.	*page 7-349*
nat-pool-config-instance	Invokes NAT pool configuration parameters	*page 7-355*

7.1.37.1 ip

ip

Configures IPv4 routing components, such as default gateway, DHCP, DNS server forwarding, name server, domain name, routing standards, etc.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
ip [default-gateway|dhcp|dns-server-forward|domain-lookup|domain-name|igmp|name-server|nat|route|routing]

ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcp-client <1-1800>|static-route <1-1800>]]

ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>|routing]

ip dhcp client [hostname|persistent-lease]

ip igmp snooping {fast-leave|forward-unknown-multicast|querier}
ip igmp snooping {fast-leave|forward-unknown-multicast}
ip igmp snooping {querier} {max-response-time <1-25>|query-interval <1-18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-3>}
```

NOTE: The command 'ip igmp snooping' can be configured under bridge VLAN context also. For example: rfs7000-37FABE(config-device 00-15-70-37-FA-BE-bridge-vlan-1)#ip igmp snooping forward-unknown-multicast

```
ip nat [crypto|inside|outside|pool]

ip nat [crypto source pool|pool] <NAT-POOL-NAME>

ip nat [inside|outside] [destination|source]

ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]

ip nat [inside|outside] source [list|static]

ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]

ip nat [inside|outside] source list <IP-ACCESS-LIST-NAME> interface [<INTERFACE-NAME>|pppoe1|vlan <1-4094>|wwan1] [(address <IP>|interface <L3-IF-NAME>|overload|pool <NAT-POOL-NAME>)]

ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

```
• ip default-gateway [<IP>|<HOST-ALIAS-NAME>|failover|priority [dhcp-client <1-1800>|static-route <1-1800>]]
```

ip	Configures IPv4 routing components

default-gateway	Configures default gateway (next-hop router) parameters
<IP>	Configures default gateway's IP address • <IP> – Specify the default gateway's IP address.
failover	Configures failover to the gateway (with next higher priority) when the current default gateway is unreachable (In case of multiple default gateways). This option is enabled by default.
<HOST-ALIAS-NAME>	Configures the host alias mapped to the required default gateway • <HOST-ALIAS-NAME> – Specify the host alias name (should be existing and configured). Host alias names begin with a '*$*'.
priority [dhcp-client <1-1800>| static-route <1-1800>]	Configures default gateway priority • dhcp-client <1-1800> – Defines a priority for the default gateway acquired by the DHCP client on the VLAN interface. The default setting is 1000. • static-route <1-1800> – Defines the weight (priority) assigned to this static route versus others that have been defined to avoid potential congestion. The default setting is 100. The following keyword is common to 'dhcp-client' and 'static-route' parameters: • <1-1800> – Specify the priority from 1 - 18000 (lower the value higher is the priority).

• `ip [dns-server-forward|domain-lookup|domain-name <DOMAIN-NAME>|name-server <IP>|routing]`

ip	Configures IPv4 routing components
dns-server-forward	Enables DNS forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network. This option is disabled by default.
domain-lookup	Enables domain lookup. When enabled, human friendly domain names are converted into numerical IP destination addresses. The option is enabled by default.
domain-name <DOMAIN-NAME>	Configures a default domain name • <DOMAIN-NAME> – Specify a name for the DNS (should not exceed 64 characters in length).
name-server <IP>	Configures the name server's IP address • <IP> – Specify the IP address of the name server.
routing	Enables IP routing of logically addressed packets from their source to their destination. IPv4 routing is enabled by default.

• `ip dhcp client [hostname|persistent-lease]`

ip	Configures IPv4 routing components
dhcp	Configures the DHCP client and host
client [hostname| persistent-lease]	Sets the DHCP client • hostname – Includes the hostname in the DHCP lease for the requesting client. This option is enabled by default. • persistent-lease – Retains the last lease across reboots if the DHCP server is unreachable. A persistent DHCP lease assigns the same IP address and other network information to the device each time it renews its DHCP lease. This option is disabled by default.

- `ip igmp snooping {fast-leave|forward-unknown-multicast}`

ip	Configures IPv4 routing components
fats-leave	Optional. Enables fast leave processing. When enabled, leave messages are processed quickly, preventing the host from receiving further traffic. Should be configured for one (wired) host network only. This option is disabled by default. This feature is supported only on the AP7502, AP8232, AP8533 model access points.
igmp snooping forward-unknown-multicast	Optional. Enables unknown multicast data packets to be flooded in the specified VLAN. This option is disabled by default.

- `ip igmp snooping {querier} {max-response-time <1-25>|query-interval <1-18000>| robustness-variable <1-7>|timer expiry <60-300>|version <1-3>}`

ip	Configures IPv4 routing components
igmp snooping querier	Optional. Enables the IGMP querier functionality for the specified VLAN. By default IGMP snooping querier is disabled.
max-response-time <1-25>	Configures the IGMP maximum query response interval used in IGMP V2/V3 queries for the given VLAN. The default is 10 seconds.
query-interval <1-18000>	Configures the IGMP querier query interval in seconds. Specify a value from 1 - 18000 seconds. The default is 60 seconds.
robustness-variable <1-7>	Configures the IGMP robustness variable from 1 - 7. The default is 2.
timer expiry <60-300>	Configures the other querier time out value for the given VLAN. The default is 60 seconds.
version <1-3>	Configures the IGMP query version for the given VLAN. The default is 3.

- `ip nat [crypto source pool|pool <NAT-POOL-NAME>]`

ip	Configures IPv4 routing components
nat	Configures the NAT parameters
crypto source pool <NAT-POOL-NAME>	Configures the NAT source address translation settings for IPSec tunnels • <NAT-POOL-NAME> – Specify a NAT pool name.
pool <NAT-POOL-NAME>	Configures a pool of IP addresses for NAT • <NAT-POOL-NAME> – Specify a name for the NAT pool.

- `ip nat [inside|outside] destination static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-IP> {<1-65535>})]`

ip	Configures IPv4 routing components
nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside address translation for the destination • inside – Configures inside address translation • outside – Configures outside address translation

destination static <ACTUAL-IP>	The following keywords are common to the 'inside' and 'outside' parameters:
	• destination – Specifies destination address translation parameters
	  • static – Specifies static NAT local to global mapping
	  • <ACTUAL-IP> – Specify the actual outside IP address to map.

<1-65535> [tcp|udp]	• <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535. • tcp – Configures *Transmission Control Protocol* (TCP) port • udp – Configures *User Datagram Protocol* (UDP) port
<NATTED-IP> <1-65535>	Enables configuration of the outside natted IP address • <NATTED-IP> – Specify the outside natted IP address. • <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

```
• ip nat [inside|outside] source static <ACTUAL-IP> <1-65535> [tcp|udp] [(<NATTED-
IP> {<1-65535>})]
```

ip	Configures IPv4 routing components
nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside address translation for the source • inside – Configures inside address translation • outside – Configures outside address translation
source static <ACTUAL-IP>	The following keywords are common to the' inside' and 'outside' parameters: • source – Specifies source address translation parameters • static – Specifies static NAT local to global mapping • <ACTUAL-IP> – Specify the actual inside IP address to map.
<1-65535> [tcp|udp]	• <1-65535> – Configures the actual outside port. Specify a value from 1 - 65535. • tcp – Configures *Transmission Control Protocol* (TCP) port • udp – Configures *User Datagram Protocol* (UDP) port
<NATTED-IP> <1-65535>	Enables configuration of the outside natted IP address • <NATTED-IP> – Specify the outside natted IP address. • <1-65535> – Optional. Configures the outside natted port. Specify a value from 1 - 65535.

```
• ip nat [inside|outside] source list <IP-ACCESS-LIST-NAME> interface [<INTERFACE-
NAME>|pppoe1|vlan <1-4094>|wwan1] [(address <IP>|interface <L3-IF-NAME>|overload|
pool <NAT-POOL-NAME>)]
```

ip	Configures IPv4 routing components
nat	Configures the NAT parameters
[inside|outside]	Configures inside and outside IP access list
source list <IP-ACCESS-LIST-NAME>	Configures an access list describing local addresses • <IP-ACCESS-LIST-NAME> – Specify a name for the IP access list.
interface [<INTERFACE-NAME>| pppoe1| vlan <1-4094>| wwan1]	Selects an interface to configure. Select a layer 3 router interface or a VLAN interface. • <INTERFACE-NAME> – Selects a layer 3 interface. Specify the layer 3 router interface name. • vlan – Selects a VLAN interface • <1-4094> – Set the SVI VLAN ID of the interface. • pppoe1 – Selects PPP over Ethernet interface • wwan1 – Selects Wireless WAN interface
address <IP>	The following keyword is recursive and common to all interface types: • address <IP> – Configures the interface IP address used with NAT

interface <L3-IF-NAME>	The following keyword is recursive and common to all interface types: • interface <L3-IF-NAME> – Configures a wireless controller or service platform's VLAN interface • <L3IFNAME> – Specify the SVI VLAN ID of the interface.
overload	The following keyword is recursive and common to all interface types: • overload – Enables use of global address for many local addresses
pool <NAT-POOL-NAME>	The following keyword is recursive and common to all interface types: • pool <NAT-POOL-NAME> – Specifies the NAT pool • <NAT-POOL-NAME> – Specify the NAT pool name.

- `ip route <IP/M> [<IP>|<HOST-ALIAS-NAME>]`

ip	Configures IPv4 routing components
route	Configures the static routes
<IP/M>	Specify the IP destination prefix in the A.B.C.D/M format.
<IP>	Specify the IP address of the gateway.
<HOST-ALIAS-NAME>	Configures the host alias mapped to the required default gateway • <HOST-ALIAS-NAME> – Specify the host alias name (should be existing and configured). Host alias names begin with a '*$*'.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#ip default-gateway 172.16.10.4
rfs6000-37FABE(config-profile-default-rfs6000)#ip dns-server-forward
rfs6000-37FABE(config-profile-default-rfs6000)#ip nat inside source list test
interface vlan 1 pool pool1 overload

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip default-gateway 172.16.10.4
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 ......................................................
  qos trust 802.1p
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 ip dns-server-forward
 ip nat inside source list test interface vlan1 pool pool1 overload
  service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

```
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#?
Nat Policy Mode commands:
  address  Specify addresses for the nat pool
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-default-rfs7000-nat-pool-pool1)
```

Related Commands

no	Disables or reverts settings to their default

7.1.37.2 nat-pool-config-instance

- *ip*

Use the config-profile-<DEVICE-PROFILE-NAME> instance to configure *Network Address Translation* (NAT) pool settings.

The following example uses the config-profile-default-rfs7000 instance to configure NAT pool settings:

```
rfs6000-37FABE(config-profile-default-rfs6000)#ip nat pool pool1
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#

rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#?
Nat Policy Mode commands:
  address  Specify addresses for the nat pool
  no       Negate a command or set its defaults

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)
```

The following table summarizes NAT pool configuration commands:

Command	Description	Reference
address	Configures NAT pool addresses	*page 7-356*
no	Negates a command or sets its default	*page 7-357*

7.1.37.2.1 address

nat-pool-config-instance

Configures NAT pool of IP addresses

Define a range of IP addresses hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
address [<IP>|range <START-IP> <END-IP>]
```

Parameters

- `address [<IP>|range <START-IP> <END-IP>]`

address <IP>	Adds a single IP address to the NAT pool
range <START-IP> <END-IP>	Adds a range of IP addresses to the NAT pool • <START-IP> – Specify the starting IP address of the range. • <END-IP> – Specify the ending IP address of the range.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#address range 172.
16.10.2 172.16.10.8

rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#show context
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#
```

Related Commands

no	Removes address(es) configured with this NAT pool

7.1.37.2.2 no

nat-pool-config-instance

Removes address(es) configured with this NAT pool

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
no address [<IP>|range <START-IP> <END-IP>]
```

Parameters

- `no address [<IP>|range <START-IP> <END-IP>]`

no address [<IP>| range <START-IP> <END-IP>]	Removes a single IP address or a range of IP addresses from this NAT pool

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#show context
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#

rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#no address range 1
72.16.10.2 172.16.10.8

rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#show context
 ip nat pool pool1
rfs6000-37FABE(config-profile-default-rfs6000-nat-pool-pool1)#
```

Related Commands

address	Configures NAT pool IP address(es)

7.1.38 ipv6

Profile Config Commands

Configures IPv6 routing components, such as default gateway, DNS server forwarding, name server, routing standards, etc.

These IPv6 settings are applied to all devices using this profile.

You can also configure IPv6 settings on a device, using the device's configuration mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

NOTE: The IPv6 settings configured at the profile/device level are global configuration settings and not interface-specific.

Syntax

```
ipv6 [default-gateway|dns-server-forward|hop-limit|mld|name-server|nd-reachable-
time|neighbor|ns-interval|ra-convert|route|ula-reject-route|unicast-routing]

ipv6 [default-gateway <IPv6> {vlan <VLAN-ID>}|dns-server-forward|hop-limit <1-
255>|name-server <IPv6>|nd-reachable-time <5000-3600000>|ns-interval <1000-
3600000>|ula-reject-route|unicast-routing]

ipv6 ra-convert {throttle interval <3-1800> max-RAs <1-256>}

ipv6 mld snooping {forward-unknown-multicast|querier}
ipv6 mld snooping {forward-unknown-multicast}
ipv6 mld snooping {querier} {max-response-time <1-25000>|query-interval <1-
18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-2>}

ipv6 neighbor [<IPv6>|timeout]

ipv6 neighbor <IPv6> <MAC> [<INTF-NAME>|pppoe1|vlan <1-4094>|wwan1] {dhcp-server|
router}
ipv6 neighbor timeout <15-86400>

ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-
ID>}
```

Parameters

```
• ipv6 [default-gateway <IPv6> {vlan <VLAN-ID>}|dns-server-forward|hop-limit <1-
255>|name-server <IPv6>|nd-reachable-time <5000-3600000>|ns-interval <1000-
3600000>|ula-reject-route|unicast-routing]
```

ipv6	Configures IPv6 routing components
default-gateway <IPv6> {vlan <VLAN-ID>}	Configures IPv6 default gateway's address in the ::/0 format • vlan <VLAN-ID> – Optional. Specify the VLAN interface's ID through which the default gateway is accessible.
dns-server-forward	Enables DNS server forwarding. This command enables the forwarding of DNS queries to DNS servers outside of the network. This feature is disabled by default.

hop-limit <1-255>	Configures the IPv6 hop count limit • <1-255> – Specify a value between 1 - 255. The default is 64.
name-server <IPv6>	Configures the IPv6 name server's address • <IPv6> – Specify the address of the IPv6 name server.
nd-reachable-time <5000-3600000>	Configures the time, in milliseconds, that a neighbor is assumed to be reachable after having received *neighbor discovery* (ND) confirmation for their reachability • <5000-3600000> – Specify a value from 5000 - 3600000 milliseconds. The default is 30,000 milliseconds.
ns-interval <1000-3600000>	Configures the interval, in milliseconds, between two consecutive retransmitted *neighbor solicitation* (NS) messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address. • <1000-3600000> – Specify a value from 1000 - 3600000. The default is 1000 milliseconds.
ula-reject-route	Installs a "reject" route for *Unique Local Address* (ULA) prefixes. This ensures that site-border routers and firewalls do not forward packets with ULA source or destination addresses outside of the site, unless explicitly configured with routing information about specific /48 or longer Local IPv6 prefixes. This option is disabled by default. The ULA is an IPv6 address used in private networks for local communication within a site (for example a company, campus, or within a set of branch office networks). These site local addresses are IPv6 addresses that fall in the block fc00::/7, defined in RFC 4193.
unicast-routing	Enables IPv6 unicast routing. This feature is enabled by default.

- `ipv6 ra-convert {throttle interval <3-1800> max-RAs <1-256>}`

ipv6	Configures IPv6 routing components
ra-convert {throttle interval <3-1800> max-RAs <1-256>	Enables conversion of multicast *router advertisements* (RAs) to unicast RAs at the dot11 layer. This feature is disabled by default. • throttle – Optional. Throttles multicast RAs before converting to unicast • interval <3-1800> – Throttles multicast RAs for a specified time period. Specify the interval from 3 - 1800 seconds. The default is 3 seconds. • max-RAs <1-256> – Specifies the maximum number of RAs per IPv6 router during the specified throttle interval. Specify a value from 1 - 256. The default is 1.

- `ipv6 mld snooping {forward-unknown-multicast}`

ipv6	Configures IPv6 routing components
mld snooping forward-unknown-multicast	Enables *multicast listener discovery* (MLD) protocol snooping. This feature is disabled by default. When enabled, IPv6 devices (access point, wireless controller, or service platform) can examine MLD messages exchanged between hosts and multicast routers to discern which hosts are receiving multicast group traffic. Based on the information gathered these devices forward multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces. This prevents VLANs from getting flooded with IPv6 multicast traffic. Contd..

	• forward-unknown-multicast – Optional. Enables unknown multicast forwarding. This feature is enabled by default.

• `ipv6 mld snooping {querier} {max-response-time <1-25000>|query-interval <1-18000>|robustness-variable <1-7>|timer expiry <60-300>|version <1-2>}`

ipv6	Configures IPv6 routing components
mld snooping querier	Enables MLD protocol snooping • querier – Optional. Enables the on-board MLD querier. When enabled, IPv6 devices send query messages to discover which network devices are members of a given multicast group.This option is disabled by default.
max-response-time <1-25000>	Configures the MLD querier's maximum query response time. This is the time for which the querier waits before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. • <1-25000> – Specify a value from 1 - 25000 milliseconds. The default is 10 milliseconds.
query-interval <1-18000>	Configures the interval, in seconds, between two consecutive MLD querier's queries The robustness variable is an indication of how susceptible the subnet is to lost packets. MLD can recover from robustness variable minus 1 lost MLD packets. • <1-18000> – Specify a value from 1 - 18000 seconds. The default is 60 seconds.
robustness-variable <1-7>	Configures the MLD IGMP robustness variable. This value is used by the sender of a query. • <1-7> – Select a value from 1 - 7. The default is 2.
timer expiry <60-300>	Configures the MLD other querier (any external querier) timeout • <60-300> – Specify a value from 60 - 300 seconds. The default is 60 seconds.
version <1-2>	Configures the MLD querier's version. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. • <1-2> – Select the MLD version from 1 - 2. The default is 2.

• `ipv6 neighbor <IPv6> <MAC> [<INTF-NAME>|pppoe1|vlan <1-4094>|wwan1] {dhcp-server|router}`

ipv6	Configures IPv6 routing components
neighbor	Configures static IPv6 neighbor entries
<IPv6>	Specify the IPv6 address for which a static neighbor entry is created.
<MAC>	Specify the MAC address associated with the specified IPv6 address.
[<INTF-NAME>| pppoe1| vlan <1-4094>| wwan1]	Specify the following interface settings: • <INTF-NAME> – Selects the layer 3 router interface. Specify the interface name. • pppoe1 – Selects the PPP over Ethernet interface • vlan <1-4094> – Selects the VLAN interface. Specify the VLAN interface index. • wwan1 – Selects the wireless WAN interface
{dhcp-server|router}	After specifying interface type, you can optionally specify the device type for this neighbor solicitation. • dhcp-server – Optional. States this neighbor entry is for a DHCP server • router – Optional. States this neighbor entry is for a router

- `ipv6 neighbor timeout <15-86400>`

neighbor	Configures static IPv6 neighbor entries
timeout <15-86400>	Configures the timeout, in seconds, for the static neighbor entries • <15-86400> – Specify a value from 15 - 86400 seconds. The default is 3600 seconds.

- `ipv6 route <DEST-IPv6-PREFIX/PREFIX-LENGTH> <IPv6-GATEWAY-ADDRESS> {vlan <VLAN-ID>}`

ipv6	Configures IPv6 routing components
route	Configures the static routes These routes are maintained in the IPv6 *Forwarding Information Base* (FIB). To view FIB6 routing entries, use the *service > show fib6 > <TABLE-ID>* command.
<DEST-IPv6-PREFIX/ PREFIX-LENGTH>	Specify the IPv6 destination prefix (IPV6 network) and the prefix length.
<IPv6-GATEWAY-ADDRESS>	Specify the IPv6 gateway's address.
vlan <VLAN-ID>	Optional. specify the VLAN interface's ID (through which the defalut gateway is accessible) This parameter is needed only if the gateway address is a link local address.

Example

```
rfs6000-81742D(config-profile-TestRFS6000)#ipv6 default-gateway
2001:10:10:10:10:10:10:2

rfs6000-81742D(config-profile-TestRFS6000)#ipv6 dns-server-forward

rfs6000-81742D(config-profile-TestRFS6000)#ipv6 mld snooping

rfs6000-81742D(config-profile-TestRFS6000)#show context
profile rfs6000 TestRFS6000
 ipv6 mld snooping
 ipv6 dns-server-forward
 ipv6 default-gateway 2001:10:10:10:10:10:10:2
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 --More--
rfs6000-81742D(config-profile-TestRFS6000)#
```

Related Commands

no	Disables or reverts IPv6 settings to their default

7.1.39 l2tpv3

Profile Config Commands

Defines the L2TPV3 settings for tunneling layer 2 payloads using VPNs

L2TPv3 is an IETF standard that defines the control and encapsulation protocol settings for tunneling layer 2 frames in an IP network (and access point profile) between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables WiNG supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between WiNG devices and other vendor devices supporting the L2TPv3 protocol.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|logging|manual-session|router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port <1024-65535>]

l2tpv3 logging ip-address [<IP>|any] hostname [<HOSTNAME>|any] router-id [<IP>|<WORD>|any]
```

Parameters

- `l2tpv3 [hostname <HOSTNAME>|inter-tunnel-bridging|manual-session|router-id [<1-4294967295>|<IP>]|tunnel|udp-listen-port <1024-65535>]`

l2tpv3	Configures the L2TPv3 protocol settings for a profile
hostname <HOSTNAME>	Configures the host name sent in the L2TPv3 signalling messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host. • <HOSTNAME> – Specify the L2TPv3 specific host name.
inter-tunnel-bridging	Enables inter tunnel bridging of packets. This feature is disabled by default.
manual-session	Creates/modifies L2TPv3 manual sessions For more information, see *l2tpv3-manual-session-commands*.
router-id [<1-4294967295>|<IP>]	Configures the router ID sent in the L2TPv3 signaling messages. These signaling (AVP) messages help to identify tunneled peers. • <1-4294967295> – Configures the router ID in decimal format from 1 - 4294967295 • <IP> – Configures the router ID in the IP address (A.B.C.D) format
tunnel	Creates/modifies a L2TPv3 tunnel For more information, see *l2tpv3-tunnel-commands*.
udp-listen-port <1024-65535>	Configures the UDP port used to listen for incoming traffic • <1024-65535> – Specify the UDP port from 1024 - 65535 (default is 1701)

- `l2tpv3 logging ip-address [<IP>|any] hostname [<HOSTNAME>|any] router-id [<IP>|<WORD>|any]`

l2tpv3	Configures L2TPv3 protocol settings for a profile

logging	Enables L2TPv3 tunnel event logging and debugging. When enabled, all events relating to Ethernet frames to and from bridge VLANs and physical ports on a specified IP address, host or router ID are logged. This option is disabled by default.
ip-address [<IP>|any]	Configures the L2TPv3 peer tunnel IP address for which event logging is enabled. The options are: • <IP> – Specify the peer's IP address. L2TPv3 events are captured and logged for the specified peer. • any – Peer's IP address is not specified. Enables event logging for all incoming connections from any IP address.
hostname [<HOSTNAME>| any]	Configures the L2TPv3 peer tunnel hostname for which event logging is enabled. The options are: • <HOSTNAME> – Specify the peer's host name. L2TPv3 events are captured and logged for specified host. • any – Peer's hostname is not specified. Enables debugging for all incoming connections from any host.
router-id [<IP>|<WORD>|any]	Configures the L2TPv3 tunnel router ID for which event logging is enabled. The options are: • <IP> – Specify the router ID in the IP address format. • <WORD> – Specify the router ID in the form of an integer or range. For example 100-200. • any – Router ID is not specified. Enables debugging for all incoming connections from any L2TPv3 router.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#l2tpv3 hostname l2tpv3Host1

rfs6000-37FABE(config-profile-default-rfs6000)#l2tpv3 inter-tunnel-bridging

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ..............................................
  l2tpv3 hostname l2tpv3Host1
 l2tpv3 inter-tunnel-bridging
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Negates a L2TPv3 tunnel settings on this profile

7.1.40 l3e-lite-table

Profile Config Commands

Configures L3e lite table aging time

The L3e Lite table stores information about destinations and their location within a specific IPSec tunnel. This enables quicker packet transmissions. The table is updated as nodes transmit packets.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
l3e-lite-table aging-time <10-1000000>
```

Parameters

- `l3e-lite-table aging-time <10-1000000>`

l3e-lite-table aging-time <10-1000000>	Configures the aging time in seconds. The aging time defines the duration a learned L3e entry (IP, VLAN) remains in the L3e Lite table before deletion due to lack of activity. The default is 300 seconds.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#l3e-lite-table aging-time 1000

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs7000 default-rfs7000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
.....................................................
  interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 l3e-lite-table aging-time 1000
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Removes the L3e lite table aging time configuration

7.1.41 led

Profile Config Commands

Turns on and off access point LEDs

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
led {flash-pattern}
```

Parameters

- `led {flash-pattern}`

led flash-pattern	Optional. Enables LED flashing on the device using this profile Select this option to flash an access point's LEDs in a distinct manner (different from its operational LED behavior). Enabling this feature allows an administrator to validate an access point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.

Example

```
rfs6000-37FABE(config-profile-RFS6000Test)#led flash-pattern

rfs6000-37FABE(config-profile-RFS6000Test)#show context
profile rfs6000 RFS6000Test
 no autoinstall configuration
 no autoinstall firmware
 led flash-pattern
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 --More--
rfs6000-37FABE(config-profile-RFS6000Test)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.42 led-timeout

Profile Config Commands

Configures the LED-timeout timer in the device or profile configuration mode

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
led-timeout [<15-1440>|shutdown]
```

Parameters

- `led-timeout [<15-1440>|shutdown]`

led-time [<15-1440>| shutdown]	Sets the LED-timeout timer. The value provided here determines the interval (time to lapse) for which a device's LEDs are turned off after the last radio state change. For example, if set at 15 minutes, the LEDs are turned off for 15 minutes after the last radio state change. • <15-1440> – Specify a value from 15 - 1400 minutes. The default is 30 minutes. • shutdown – Shuts down the LED-timeout timer. The device LEDs are not turned off.

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout 25

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
 no autogen-uniqueid
 ip default-gateway 192.168.13.2
 led-timeout 25
 --More--
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#led-timeout shutdown

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 license AAP
66069c24b3bb1259b34ff016c723a9e299dd408f0ff891e7c5f7e279a382648397d6b3e975e356a1
 license HTANLT
66069c24b3bb1259eb36826cab3cc83999dd408f0ff891e74b62b2d3594f0b3dde7967f30e49e497
 no autogen-uniqueid
 ip default-gateway 192.168.13.2
 led-timeout shutdown
 crypto ikev2 peer IKEv2Peer1
--More--
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands

no	Disables LED-timeout timer

7.1.43 legacy-auto-downgrade

Profile Config Commands

Enables device firmware to auto downgrade when legacy devices are detected

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
legacy-auto-downgrade
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#legacy-auto-downgrade
```

Related Commands

no	Prevents device firmware from auto downgrading when legacy devices are detected

7.1.44 legacy-auto-update

Profile Config Commands

Auto updates an AP7161 legacy access point firmware

Supported in the following platforms:

- Access Points — AP7161

Syntax

```
legacy-auto-update ap71xx image <FILE>]
```

Parameters

- `legacy-auto-update ap71xx image <FILE>`

legacy-auto-update	Updates a legacy AP7161 access point firmware
ap71xx image <FILE>	Auto updates legacy AP7161 firmware • image – Sets the path to the firmware image • <FILE> – Specify the path and filename in the flash:/ap.img format.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#legacy-auto-update ap71xx image
flash:/ap47d.img
```

Related Commands

no	Disables automatic legacy firmware upgrade

7.1.45 lldp

Profile Config Commands

Enables LLDP on this profile and configures LLDP settings

LLDP or IEEE 802.1AB is a vendor-neutral Data Link Layer protocol used by network devices for advertising of (announcing) identity, capabilities, and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery. Both LLDP snooping and ability to generate and transmit LLDP packets is provided.

Information obtained via CDP and LLDP snooping is available in the UI. Information obtained using LLDP is provided during the adoption process, so the layer 2 device detected by the access point can be used as a criteria in the provisioning policy.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
lldp [holdtime|med-tlv-select|run|timer]

lldp [holdtime <10-1800>|run|timer <5-900>]

lldp med-tlv-select [inventory-management|power-management {auto}]
```

Parameters

- `lldp [holdtime <10-1800>|run|timer <5-900>]`

lldp	Enables LLDP on this profile and configures LLDP settings
holdtime <10-1800>	Sets the holdtime for transmitted LLDP PDUs. This command specifies the time a receiving device holds information before discarding. • <10-1800> – Specify a holdtime from 10 - 1800 seconds. The default is 180 seconds.
run	Enables LLDP on this profile
timer <5-900>	Sets the transmit interval. This command specifies the transmission frequency of LLDP updates in seconds. • <5-900> – Specify transmit interval from 5 - 900 seconds. The default is 60 seconds.

- `lldp med-tlv-select [inventory-management|power-management {auto}]`

lldp	Enables LLDP on this profile and configures LLDP settings
med-tlv-select [inventory-management| power-management {auto}]	Provides additional media endpoint device TLVs to enable inventory and power management discovery. Specifies the LLDP MED TLVs to send or receive. • inventory-management – Enables inventory management discovery. Allows an endpoint to convey detailed inventory information about itself. This information includes details, such as manufacturer, model, and software version, etc. This option is enabled by default. Contd..

	• power-management auto – Enables extended power via MDI discovery. Allows endpoints to convey power information, such as how the device is powered, power priority, etc. • auto – Optional. Assigns default value based on device type

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#lldp timer 20

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
 ........................................
 use firewall-policy default
 ip dns-server-forward
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
 ip nat inside source list test interface vlan1 pool pool1 overload
 lldp timer 20
 --More--
rfs6000-37FABE(config-profile-default-rfs7000)#
```

Related Commands

no	Disables LLDP on this profile

7.1.46 load-balancing

Profile Config Commands

Configures load balancing parameters

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
load-balancing [advanced-params|balance-ap-loads|balance-band-loads|balance-channel-loads|band-control-startegy|band-ratio|group-id|neighbor-selection-strategy]

load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load|equality-margin|hiwater-threshold|max-neighbors|max-preferred-band-load|min-common-clients|min-neighbor-rssi|min-probe-rssi]

load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load] [client-weightage|throughput-weightage] <0-100>

load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <0-100>

load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|channel-5GHz]<0-100>

load-balancing advanced-params max-preferred-band-load [2.4GHz|5GHz] <0-100>

load-balancing advanced-params [max-neighbors <0-16>|min-common-clients <0-256>|min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]

load-balancing [balance-ap-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]

load-balancing band-control-strategy [distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]

load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]

load-balancing group-id <GROUP-ID>

load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification|use-smart-rf]
```

Parameters

```
• load-balancing advanced-params [2.4GHz-load|5GHz-load|ap-load] [client-weightage|throughput-weightage] <0-100>
```

load-balancing advanced-params	Configures advanced load balancing parameters
2.4GHz-load [client-weightage| throughput-weightage] <0-100>	Configures 2.4 GHz load calculation weightages • client-weightage – Specifies weightage assigned to the client-count when calculating the 2.4 GHz load Contd..

	• throughput-weightage – Specifies weightage assigned to throughput, when calculating the 2.4 GHz load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.
5GHz-load [client-weightage| throughput-weightage] <0-100>	Configures 5.0 GHz load calculation weightages • client-weightage – Specifies weightage assigned to the client-count when calculating the 5.0 GHz load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the 5.0 GHz load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.
ap-load [client-weightage| throughput-weightage] <0-100>	Configures AP load calculation weightages • client-weightage – Specifies weightage assigned to the client-count, when calculating the AP load • throughput-weightage – Specifies weightage assigned to throughput, when calculating the AP load The following keyword is common to the 'client-weightage' and 'throughput-weightage' parameters: • <0-100> – Sets the margin as a load percentage from 1 - 100. The default client-weightage is 90%. The default throughput-weightage is 10%.

- `load-balancing advanced-params equality-margin [2.4GHz|5GHz|ap|band] <0-100>`

load-balancing advanced-params	Configures advanced load balancing parameters
equality-margin [2.4GHz|5GHz|ap| band] <0-100>	Configures the maximum load difference considered equal. The load is compared for different 2.4 GHz channels, 5.0 GHz channels, APs, or bands. • 2.4GHz – Configures the maximum load difference considered equal when comparing loads on different 2.4 GHz channels • 5GHz – Configures the maximum load difference considered equal when comparing loads on different 5.0 GHz channels • ap – Configures the maximum load difference considered equal when comparing loads on different APs • band – Configures the maximum load difference considered equal when comparing loads on different bands The following keyword is common to 2.4 GHz channels, 5.0 GHz channels, APs, and bands: • <0-100> – Sets the margin as a load percentage from 1 - 100. The default equality-margin for 2.5 GHz, 5.0 GHz, ap, and band loads is 1%.

- `load-balancing advanced-params hiwater-threshold [ap|channel-2.4GHz|channel-5GHz] <0-100>`

load-balancing advanced-params	Configures advanced load balancing parameters
hiwater-threshold	Configures the load beyond which load balancing is invoked
[ap|channel-2.4GHz|channel-5GHz] <0-100>	Select one of the following options: • ap – Configures the AP load beyond which load balancing begins • channel-2.4GHz – Configures the AP load beyond which load balancing begins (for APs on 2.4 GHz channel) • channel-5GHz – Configures the AP load beyond which load balancing begins for (APs on 5.0 GHz channel) The following keyword is common for the 'AP', 'channel-2.4GHz', and 'channel-5GHz' parameters: • <0-100> – Sets the load threshold as a number from 1 - 100. The default hiwater-threshold for channel-2.5GHz, channel-5GHz, and ap loads is 5.

- `load-balancing advanced-params max-preferred-band-load [2.4GHGz|5GHzd] <0-100>`

load-balancing advanced-params	Configures advanced load balancing parameters
max-preferred-band-load	Configures the maximum load on the preferred band, beyond which the other band is equally preferred
[2.4GHz|5GHz] <0-100>	Select one of the following options: • 2.4GHz – Configures the maximum load on 2.4 GHz, when it is the preferred band • 5GHz – Configures the maximum load on 5.0 GHz, when it is the preferred band The following keyword is common to the 2.4 GHz and 5.0 GHz bands: • <0-100> – Configures the maximum load as a percentage from 0 - 100. The default value for 2.4GHz and 5.GHz is 75%.

- `load-balancing advanced-params [max-neighbors <0-16>|min-common-clients <0-256>|min-neighbor-rssi <-100-30>|min-probe-rssi <-100-30>]`

load-balancing advanced-params	Configures advanced load balancing parameters
max-neighbors <0-16>	Configures the maximum number of confirmed neighbors to balance • <0-16> – Specify a value from 0 - 16. Optionally configure a minimum of 0 neighbors and a maximum of 16 neighbors. The default is 16.
min-common-clients <0-256>	Configures the minimum number of common clients that can be shared with the neighbor for load balancing • <0-256> – Specify a value from 0 - 256. Optionally configure a minimum of 0 clients and a maximum of 256 clients. The default is 0.
min-neighbor-rssi <-100-30>	Configures the minimum signal strength (RSSI) of a neighbor detected • <-100-30> – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -65 dBm.

min-probe-rssi <-100-30>	Configures the minimum received probe signal strength required to qualify the sender as a common client • <0-100> – Sets the signal strength in dBm. Specify a value from -100 - 30 dBm. The default is -100 dBm.

- `load-balancing [balance-ap-loads|balance-band-loads|balance-channel-loads [2.4GHz|5GHz]]`

load-balancing	Configures the following load balancing parameters: ap-loads, band-loads, and channel-loads.
balance-ap-loads	Enables neighbor AP load balancing. This option distributes the access point's radio load amongst other controller managed access point radios. This option is disabled by default.
balance-band-loads	Enables balancing of the total band load amongst neighbors. This option balances the access point's radio load by assigning a ratio to both the 2.4 GHz and 5.0 GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 GHz or 5.0 GHz band. This option is disabled by default.
balance-channel-loads [2.4GHz|5GHz]	Enables the following: • 2.4GHz – Channel load balancing on 2.4 GHz band. This option is disabled by default. Balances the access point's 2.4 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 2.4 GHz radio if a channel is over utilized. • 5GHz – Channel load balancing on 5.0 GHz band. This option is disabled by default. Balances the access point's 5.0 GHz radio load across channels supported within the country of deployment. This can prevent congestion on the 5.0 GHz radio if a channel is over utilized.

- `load-balancing band-control-strategy [distribute-by-ratio|prefer-2.4GHz|prefer-5GHz]`

load-balancing band-control-strategy	Configures a band control strategy By default, this option steers 5.0 GHz-capable clients to the 5.0 GHz band. When an access point hears a request from a client to associate on both the 2.4 GHz and 5.0 GHz bands, it knows the client is capable of operation in 5.0 GHz. Band steering steers the client by responding only to the 5.0 GHz association request and not the 2.4 GHz request. Consequently, the client only associates in the 5.0 GHz band.
distribute-by-ratio	Distributes clients to either band according to the band-ratio
prefer-2.4GHz	Nudges all dual-band clients to 2.4 GHz band
prefer-5GHz	Nudges all dual-band clients to 5.0 GHz band. This is the default setting.

- `load-balancing band-ratio [2.4GHz|5GHz] [0|<1-10>]`

load-balancing band-ratio	Configures the relative loading of 2.4 GHz band and 5.0 GHz band.This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz or the radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz or 5.0 GHz radio band.
2.4GHz [0|<1-10>]	Configures the relative loading of 2.4 GHz band • 0 – Selecting '0' steers all dual-band clients preferentially to the other band • <0-10> – Configures a relative load as a number from 0 - 10. The default is 0.

5ghz [0|<1-10>]	Configures the relative loading of 5.0 GHz band • 0 – Selecting '0' steers all dual-band clients preferentially to the other band • <0-10> – Configures a relative load as a number from 0 - 10. The default is 1.

- `load-balancing group-id <GROUP-ID>`

load-balancing group-id <GROUP-ID>	Configures group ID to facilitate load balancing • <GROUP-ID> – Specify the group ID. This option is enabled only when a group ID is configured.

- `load-balancing neighbor-selection-strategy [use-common-clients|use-roam-notification|use-smart-rf]`

load-balancing neighbor-selection-strategy	Configures a neighbor selection strategy. The options are: use-common-clients, use-roam-notification, and use-smart-rf
use-common-clients	Selects neighbors based on probes from clients common to neighbors. This option is enabled by default.
use-roam-notification	Selects neighbors based on roam notifications from roamed clients. This option is enabled by default.
use-smart-rf	Selects neighbors detected by Smart RF. This option is enabled by default.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#load-balancing advanced-params
2.4ghz-load throughput-weightage 90

rfs6000-37FABE(config-profile-default-rfs6000)#load-balancing advanced-params
hiwater-threshold ap 90

rfs6000-37FABE(config-profile-default-rfs6000)#load-balancing balance-ap-loads

rfs7000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ip default-gateway 172.16.10.4
 autoinstall configuration
 autoinstall firmware
 load-balancing advanced-params 2.4ghz-load throughput-weightage 90
 load-balancing advanced-params hiwater-threshold ap 90
 load-balancing balance-ap-loads
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables load balancing on this profile

7.1.47 logging

Profile Config Commands

Enables message logging and configures logging settings. When enabled, the profile logs individual system events to a user-defined log file or a syslog server. Message logging is disabled by default.

Enabling message logging is recommended, because system event logs can be analyzed to determine an overall pattern that may be negatively impacting performance.

This command can also be executed in the device configuration mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
logging [aggregation-time|buffered|console|facility|forward|host|on|syslog]

logging [aggregation-time <1-60>|host [<IPv4>|<IPv6>] {port <1-65535>}|on]

logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical|
errors|warnings|notifications|informational|debugging]

logging facility [local0|local1|local2|local3|local4|local5|local6|local7]
```

Parameters

- `logging [aggregation-time <1-60>|host [<IPv4>|<IPv6>] {port <1-65535>}|on]`

logging	Enables message logging and configures logging settings
aggregation-time <1-60>	Sets the number of seconds for aggregating repeated messages. This is the interval at which system events are logged on behalf of this profile. The shorter the interval, the sooner the event is logged. • <1-60> – Specify a value from 1 - 60 seconds. The default value is 0.
host [<IPv4>|<IPv6>] {port <1-65535>}	Configures a remote host to receive log messages. Defines numerical (non DNS) IPv4 or IPv6 addresses for external resources where logged system events can be sent on behalf of the profile (or device). A maximum of four entries can be made. • <IPv4> – Specify the IPv4 address of the remote host. • <IPv6> – Specify the IPv6 address of the remote host. • port <1-65535> – Optional. Configures the syslog port • <1-65535> – Specify the syslog port from 1 - 65535. The default port is 514.
on	Enables the logging of system messages

- `logging [buffered|console|syslog|forward] [<0-7>|emergencies|alerts|critical|errors|warnings|notifications|informational|debugging]`

logging	Enables message logging and configures logging settings
buffered	Sets the buffered logging level
console	Sets the console logging level
syslog	Sets the syslog server's logging level

forward	Forwards system debug messages to the wireless controller or service platform
[<0-7>|alerts| criticail|debugging| emergencies|errors| informational| notifications| warnings]	The following keywords are common to the buffered, console, syslog, and forward parameters. All incoming messages have different severity levels based on their importance. The severity level is fixed on a scale of 0 - 7. • <0-7> – Sets the message logging severity level on a scale of 0 - 7 • emergencies – Severity level 0: System is unusable • alerts – Severity level 1: Requires immediate action • critical – Severity level 2: Critical conditions • errors – Severity level 3: Error conditions • warnings – Severity level 4: Warning conditions (default) • notifications – Severity level 5: Normal but significant conditions • informational – Severity level 6: Informational messages • debugging – Severity level 7: Debugging messages

- `logging facility [local0|local1|local2|local3|local4|local5|local6|local7]`

logging	Enables message logging and configures logging settings
facility [local0|local1| local2|local3|local4| local5|local6|local7]	Enables the syslog to decide where to send the incoming message There are 8 logging facilities, from syslog0 to syslog7. • local0 – Syslog facility local0 • local1 – Syslog facility local1 • local2 – Syslog facility local2 • local3 – Syslog facility local3 • local4 – Syslog facility local4 • local5 – Syslog facility local5 • local6 – Syslog facility local6 • local7 – Syslog facility local7

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#logging facility local4

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
 ................................................
 ip dns-server-forward
 logging facility local4
 ip nat pool pool1
  address range 172.16.10.2 172.16.10.8
 ip nat inside source list test interface vlan1 pool pool1 overload
 lldp timer 20
  service pm sys-restart
 router ospf
 l2tpv3 hostname l2tpv3Host1
 l2tpv3 inter-tunnel-bridging
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables logging on this profile

7.1.48 mac-address-table

Profile Config Commands

Configures the MAC address table. Use this command to create MAC address table entries by assigning a static address to the MAC address table.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mac-address-table [aging-time|detect-gateways|static]
mac-address-table aging-time [0|<10-1000000>]
mac-address-table detect-gateways
mac-address-table static <MAC> vlan <1-4094> interface [<L2-INTERFACE>|ge <1-4>|
port-channel <1-2>]
```

Parameters

- `mac-address-table aging-time [0|<10-1000000>]`

mac-address-table aging-time [0|<10-1000000>]	Sets the duration a learned MAC address persists after the last update • 0 – Entering the value '0' disables the aging time • <10-1000000> – Sets the aging time from 10 -100000 seconds. The default is 300 seconds.

- `mac-address-table detect-gateways`

mac-address-table detect-gateways	Enables automatic detection of gateways. Detected gateways are remembered in the MAC address table.

- `mac-address-table static <MAC> vlan <1-4094> interface [<L2-INTERFACE>|ge <1-4>| port-channel <1-2>]`

mac-address-table static <MAC>	Creates a static MAC address table entry • <MAC> – Specifies the static address to add to the MAC address table. Specify the MAC address in the AA-BB-CC-DD-EE-FF, AA:BB:CC:DD:EE:FF, or AABB.CCDD.EEFF format.
vlan <1-4094>	Assigns a static MAC address to a specified VLAN port • <1-4094> – Specify the VLAN index from 1 - 4094.

interface [<L2-INTERFACE>| ge <1-4>| port-channel <1-2>]	Specifies the interface type. The options are: layer 2 Interface, GigabitEthernet interface, and a port channel interface
	• <L2-INTERFACE> – Specify the layer 2 interface name.
	• ge – Specifies a GigabitEthernet interface
	  • <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
	• port-channel – Specifies a port channel interface
	  • <1-2> – Specify the port channel interface index from 1 - 2.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#mac-address-table static 00-40-96-
B0-BA-2A vlan 1 interface ge 1

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
.....................................................
  logging facility local4
 mac-address-table static 00-40-96-B0-BA-2A vlan 1 interface ge1
 ip nat pool pool1
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.49 mac-auth

Profile Config Commands

Enables authentication of a client's MAC address on wired ports. When configured, MAC authentication will be enabled on devices using this profile.

To enable MAC address authentication on a device, enter the device's configuration mode and execute the *mac-auth* command.

When enabled, the source MAC address of a device, connected to the specified wired port, is authenticated with the RADIUS server. Once authenticated the device is permitted access to the managed network and packets from the authenticated source are processed. If not authenticated the device is either denied access or provided guest access through the guest VLAN (provided guest VLAN access is configured on the port).

Enabling MAC authentication requires you to first configure a AAA policy specifying the RADIUS server. Configure the client's MAC address on the specified RADIUS server. Attach this AAA policy to a profile or a device. Finally, enable MAC authentication on the desired wired port of the device or device-profile.

Only one MAC address is supported for every wired port. Consequently, when one source MAC address is authenticated, packets from all other sources are dropped.

To enable client MAC authentication on a wired port:

1 Configure the user on the RADIUS server. The following examples create a RADIUS server user entry.
   a <DEVICE>(config)#radius-group <RAD-GROUP-NAME>

```
<DEVICE>(config-radius-group-<RAD-GROUP-NAME>)#policy vlan <VLAN-ID>
```

   b <DEVICE>(config)#radius-user-pool-policy <RAD-USER-POOL-NAME>

```
<DEVICE>(config-radius-user-pool-<RAD-USER-POOL-NAME>)#user <USER-NAME> password
<PASSWORD> group <RAD-GROUP-OF-STEP-A>
```

   Note: The <USER-NAME> and <PASSWORD> should be the client's MAC address. This address will be matched against the MAC address of incoming traffic at the specified wired port.

   c <DEVICE>(config)#radius-server-policy <RAD-SERVER-POL-NAME>

```
<DEVICE>(config-radius-server-policy-<RAD-SERVER-POL-NAME>)#use radius-user-
pool-policy <RAD-USER-POOL-OF-STEP-B>
```

2 Configure a AAA policy exclusively for wired MAC authentication and specify the authentication (RADIUS) server settings. The following example creates a AAA policy 'macauth' and enters its configuration mode:

```
<DEVICE-A>(config)#aaa-policy macauth
<DEVICE-A>(config-aaa-policy-macauth)#...
```

   a Specify the RADIUS server details.

```
<DEVICE-A>(config)#aaa-policy macauth
<DEVICE-A>(config-aaa-policy-macauth)#authentication server <1-6> [host
<IP>|onboard]
```

3 Attach the AAA policy to the device or profile. When attached to a profile, the AAA policy is applied to all devices using this profile.

```
<DEVICE>(config-device-aa-bb-cc-dd-ee)#mac-auth use aaa-policy macauth

<DEVICE>(config-profile-<DEVICE-PROFILE-NAME>)#mac-auth use aaa-policy macauth
```

4 Enable mac-auth on the device's desired GE port. When enabled on a profile, MAC address authentication is enabled, on the specified GE port, of all devices using this profile.

```
<DEVICE>(config-device-aa-bb-cc-dd-ee)#interface ge x
<DEVICE>(config-device-aa-bb-cc-dd-ee-gex)#mac-auth

<DEVICE>(config-profile-<PROFILE-NAME>)#interface ge x
<DEVICE>(config-profile-<PROFILE-NAME>)#mac-auth
```

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mac-auth use aaa-policy <AAA-POLICY-NAME>
```

Parameters

- `mac-auth use aaa-policy <AAA-POLICY-NAME>`

mac-auth	Enables 802.1X authentication of MAC addresses on this profile. Use the device configuration mode to enable this feature on a device.
use aaa-policy <AAA-POLICY-NAME>	Associates an existing AAA policy with this profile (or device) • <AAA-POLICY NAME> – Specify the AAA policy name. The AAA policy used should be created especially for MAC authentication.

Example

The following examples demonstrate the configuration of authentication of MAC addresses on wired ports:

```
rfs4000-229D58(config-aaa-policy-mac-auth)#authentication server 1 onboard
controller

rfs4000-229D58(config-aaa-policy-mac-auth)#show context
aaa-policy mac-auth
 authentication server 1 onboard controller
rfs4000-229D58(config-aaa-policy-mac-auth)#

rfs4000-229D58(config)#radius-group RG
rfs4000-229D58(config-radius-group-RG)#policy vlan 11

rfs4000-229D58(config-radius-group-RG)#show context
radius-group RF
 policy vlan 11
rfs4000-229D58(config-radius-group-RG)#

rfs4000-229D58(config)#radius-user-pool-policy RUG
rfs4000-229D58(config-radius-user-pool-RUG)#user 00-16-41-55-F8-5D password 0
0-16-41-55-F8-5D group RG

rfs4000-229D58(config-radius-user-pool-RUG)#show context
radius-user-pool-policy RUG
 user 00-16-41-55-F8-5D password 0 00-16-41-55-F8-5D group RG
rfs4000-229D58(config-radius-user-pool-RUG)#

rfs4000-229D58(config)#radius-server-policy RS
rfs4000-229D58(config-radius-server-policy-RS)#use radius-user-pool-policy RUG

rfs4000-229D58(config-radius-server-policy-RS)#show context
```

```
radius-server-policy RS
 use radius-user-pool-policy RUG
rfs4000-229D58(config-radius-server-policy-RS)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#show context
 interface ge4
  dot1x authenticator host-mode single-host
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge4)#

rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#show context
 interface ge5
  switchport mode access
  switchport access vlan 1
  dot1x authenticator host-mode single-host
  dot1x authenticator guest-vlan 5
  dot1x authenticator port-control auto
  mac-auth
rfs4000-229D58(config-device-00-23-68-22-9D-58-if-ge5)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 4
Mac Auth info for interface GE4
-----------------------------------
 Mac Auth Enabled
 Mac Auth Authorized
Client MAC 00-16-41-55-F8-5D

rfs4000-229D58(config-device-00-23-68-22-9D-58)#

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show macauth interface ge 5
Mac Auth info for interface GE5
-----------------------------------
 Mac Auth Enabled
 Mac Auth Not Authorized

rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

Related Commands

no	Disables authentication of MAC addresses on wired ports settings on this profile (or device)

7.1.50 management-server

Profile Config Commands

Configures a management server with this profile. This command is also applicable to the device configuration context.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
management-server <HOST-NAME> port <1-65535>
```

Parameters

- `management-server <HOST-NAME> port <1-65535>`

management-server <HOST-NAME> port <1-65535>	Configures a management server with this profile. Use this command to identify the management server. • <HOST-NAME> – Specify the management server's host name. • port <1-65535> – Specify the port where the management server is reachable. The default setting is port 443.

Example

```
rfs6000-81742D(config-profile-testRFS6000)#management-server nx9500-6C8809 port
300

rfs6000-81742D(config-profile-testRFS6000)#show context include-factory | include
management-server
 management-server nx9500-6C8809 port 300
rfs6000-81742D(config-profile-testRFS6000)#
```

Related Commands

no	Removes the management server configuration

7.1.51 memory-profile

Profile Config Commands

Configures memory profile used on the device

Supported in the following platforms:

- Access Points — AP6511, AP6521

Syntax

```
memory-profile [adopted|standalone]
```

Parameters

- `memory-profile [adopted|standalone]`

memory-profile	Configures memory profile used on the device
adopted	Configures adopted mode (no GUI and higher MiNT routes, firewall flows)
standalone	Configures standalone mode (GUI and fewer MiNT routes, firewall flows)

Example

```
nx9500-6C8809(config-profile-testAP6511)#memory-profile adopted
Note: memory-profile change will take effect after device reboot
nx9500-6C8809(config-profile-testAP6511)#
```

Related Commands

no	Resets device's memory profile configuration

7.1.52 meshpoint-device

Profile Config Commands

Configures meshpoint device parameters. This feature is configurable in the profile and device configuration modes.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
meshpoint-device <MESHPOINT-NAME>
```

Parameters

- `meshpoint-device <MESHPOINT-NAME>`

meshpoint-device <MESHPOINT-NAME>	Configures meshpoint device parameters • <MESHPOINT-NAME> – Specify meshpoint name.

Usage Guidelines

For *Vehicular Mounted Modem* (VMM) access points or other mobile devices, set the path selection method as mobile-snr-leaf in the config-meshpoint-device mode. For more information, see *path-method*.

Example

```
rfs6000-37FABE(config-profile-testAP7161)#meshpoint-device test

rfs6000-37FABE(config-profile-testAP7161-meshpoint-test)#?
Mesh Point Device Mode commands:
  acs           Configure auto channel selection parameters
  exclude       Exclude neighboring Mesh Devices
  hysteresis    Configure path selection SNR hysteresis values
  monitor       Event Monitoring
  no            Negate a command or set its defaults
  path-method   Path selection method used to find a root node
  preferred     Configure preferred path parameters
  root          Set this meshpoint as root
  root-select   Root selection method parameters

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-testAP7161-meshpoint-test)#
```

Related Commands

no	Removes a specified meshpoint

NOTE: For more information on the meshpoint-device configuration parameters, see *Chapter 26, MESHPOINT*.

7.1.53 meshpoint-monitor-interval

Profile Config Commands

Configures the meshpoint monitoring interval. This is the interval, in seconds, at which the meshpoint status is checked.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
meshpoint-monitor-interval <1-65535>
```

Parameters

- `meshpoint-monitor-interval <1-65535>`

meshpoint-monitor-interval <1-65535>	Configures the meshpoint monitoring interval in seconds • <1-65535> – Specify the interval from 1 - 65535 seconds. The default is 30 seconds.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#meshpoint-monitor-interval 100

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 meshpoint-monitor-interval 100
 ip default-gateway 172.16.10.4
 --More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Resets the meshpoint monitoring interval to default (30 seconds)

7.1.54 min-misconfiguration-recovery-time

Profile Config Commands

Configures the minimum device connectivity verification time

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
min-misconfiguration-recovery-time <60-3600>
```

Parameters

- `min-misconfiguration-recovery-time <60-3600>`

min-misconfiguration-recovery-time <60-3600>	Configures the minimum connectivity (with the associated device) verification interval • <60-3600> – Specify a value from 60 - 3600 seconds (default is 60 seconds).

Example

```
nx9500-6C8809(config-profile-testRFS4000)#min-misconfiguration-recovery-time 500

nx9500-6C8809(config-profile-testRFS4000)#show context
profile rfs4000 testRFS4000
 meshpoint-monitor-interval 300
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface radio1
 interface radio2
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface wwan1
 interface pppoe1
 use firewall-policy default
 min-misconfiguration-recovery-time 500
 service pm sys-restart
 router ospf
 router bgp
nx9500-6C8809(config-profile-testRFS4000)#
```

Related Commands

no	Resets setting to default (60 seconds)

7.1.55 mint

Profile Config Commands

Configures MiNT protocol parameters required for MiNT creation and adoption

MiNT links are required for adoption of a device (APs, wireless controller, and service platform) to a controller. The MiNT link is created on both the adoptee and the adopter. WiNG provides several commands to configure MiNT links and establish adoption for both IPv4 and IPv6 addresses.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mint [dis|inter-tunnel-bridging|level|link|mlcp|rate-limit|spf-latency|tunnel-across-extended-vlan|tunnel-controller-load-balancing]

mint dis [priority-adjustment <-255-255>|strict-evis-reachability]

mint inter-tunnel-bridging

mint level 1 area-id [<1-16777215>|<NUMBER-ALIAS-NAME>]

mint link [force|ip|listen|vlan]

mint link force ip [<IPv4>|<IPv6>] [<1-65535> level 2|level 2] {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-secure {gw [<IP>|<HOST-NAME>]}}

mint link [listen ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>]|vlan <1-4094>] {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-security {gw [<IP>|<HOST-NAME>]}|level [1|2]}

mint link ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>] {<1-65535>|adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-security {gw [<IP>|<HOST-NAME>]}|level [1|2]}

mint mlcp [ip|ipv6|vlan]

mint rate-limit level2 [link|mlcp]

mint rate-limit level2 [link [ip [<IPv4>|<IPv6>] <1-65535>|vlan <1-4094>]|mlcp [ip|ipv6|vlan]] rate <50-1000000> max-burst-size <2-1024> {red-threshold [background|best-effort|video|voice] <0-100>}

mint spf-latency <0-60>

mint tunnel-across-extended-vlan

mint tunnel-controller-load-balancing level1
```

Parameters

- `mint dis [priority-adjustment <-255-255>|strict-evis-reachability]`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption

dis priority-adjustment <-255-255>	Sets the relative priority for the router to become DIS (designated router) • priority-adjustment – Sets priority adjustment added to base priority The *Designated IS* (DIS) priority adjustment is the value added to the base level DIS priority to influence the DIS election. A value of +1 or greater increases DISiness. • <-255-255> – Specify a value from -255 - 255. The default is 0. Higher numbers result in higher priorities
strict-evis-reachability	Enables reaching *Ethernet Virtualization Interconnect* (EVIS) election winners through MiNT. This option is enabled by default.

- `mint inter-tunnel-bridging`

mint	Configures MiNT protocol parameters required for MiNT link creation, adoption and communication
inter-tunnel-bridging	Enables forwarding of *broadcast multicast* (BCMC) packets between devices communicating via Level 2 MiNT links. When enabled, MiNT tunnels across Level 2, adopted access points are bridged. One of the advantages of inter-tunnel bridging is the enabling of roaming between these access points. This option is disabled by default. If enabling this option, use ACLs to filter unwanted BCMC traffic.

- `mint level 1 area-id [<1-16777215>|<NUMBER-ALIAS-NAME>]`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
level 1	Configures local MiNT routing settings • 1 – Configures local MiNT routing level
area-id [<1-16777215>| <NUMBER-ALIAS-NAME>]	Specifies the level 1 routing area identifier. Use one of the following options to specify the area ID: • <1-16777215> – Specify a value from 1 - 16777215. • <NUMBER-ALIAS-NAME> – Specify a number alias (should be existing and configured). Aliases are configuration items that can be defined once and used in different configuration contexts. For more information on creating a number alias, see *alias*.

- `mint link force ip [<IPv4>|<IPv6>] [<1-65535> level 2|level 2] {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|ipsec-security {gw [<IP>|<HOST-NAME>]}}`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
link force	Creates a MiNT routing link as a forced link • force – Forces a MiNT routing link to be created even if not necessary
ip [<IPv4>|<IPv6>]	Creates a MiNT tunnel over UDP/IPv4 or IPv6 Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MINT protocol. • <IPv4> – Specify the MiNT tunnel peer's IPv4 address. • <IPv6> – Specify the MiNT tunnel peer's IPv6 address. After specifying the MiNT peer's address, configure the following MiNT link parameters: UDP port, adjacency-hold-time, cost, hello-interval, IPSec security gateway, and routing level.

<1-65535> level 2	Optional. Specifies a custom UDP port for MiNT links. Specify the port from 1 - 65535. • level – Specifies the routing level • 2 – Configures level 2 inter-site MiNT routing
adjacency-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds. The default is 46 seconds.
cost <1-100000>	Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000. The default is 100.
hello-interval <1-120>	Optional. Specifies the interval, in seconds, between successive hello packets • <1-120> – Specify a value from 1 - 120 seconds. The default is 15 seconds.
ipsec-security {gw [<IP>|<HOST-NAME>]}	Optional. Enables IPSec secure peer authentication on the MiNT link connection (link). This option is disabled by default. • gw [<IP>|<HOSTNAME>] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway's numerical IP address or administrator defined hostname.

• `mint link [listen ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>]|vlan <1-4094>] {adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|level [1|2]|ipsec-security {gw [<IP>|<HOST-NAME>]}}`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption

link listen ip [<IPv4>|<IPv6>| <HOST-ALIAS-NAME>]	Creates a MiNT routing link
	• listen – Creates a MiNT listening link
	  • ip – Creates a MiNT listening link over UDP/IP or IPv6
	  • <IPv4> – Specify the IPv4 address of the listening UDP/IP link.
	  • <IPv6> – Specify the IPv6 address of the listening UDP/IP link.
	  • <HOST-ALIAS-NAME> – Specify the host alias identifying the MiNT link address. The host alias should existing and configured.
	UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted. The typical configuration is to have a listening UDP/IP link on the IP address S.S.S.S, and for all the APs to have a regular UDP/IP link to S.S.S.S.

link vlan <1-4094>	Enables MiNT routing on VLAN • vlan – Defines a VLAN ID used by peers for inter-operation when supporting the MINT protocol. • <1-4094> – Select VLAN ID from 1 - 4094.
adjacency-hold-time <2-600>	This parameter is common to the 'listen' and 'vlan' parameters: • adjacency-hold-time <2-600> – Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds. The default is 46 seconds. For MiNT VLAN routing, the default is 13 seconds.
cost <1-100000>	This parameter is common to the 'listen' and 'vlan' parameters: • cost <1-100000> – Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000. The default is 100. For MiNT VLAN routing, the default is 10.

hello-interval <1-120>	This parameter is common to the 'listen' and 'vlan' parameters: • hello-interval <1-120> – Optional. Specifies the interval, in seconds, between successive hello packets • <1-120> – Specify a value from 1 - 120. The default is 15 seconds. For MiNT VLAN routing the default is 4 seconds.
level [1|2]	This parameter is common to the 'listen' and 'vlan' parameters: Optional. Specifies the routing levels for this routing link. The options are: • 1 – Configures local routing • 2 – Configures inter-site routing
ipsec-security {gw [<IP>| <HOST-NAME>]}	This parameter is common to the 'listen' and 'vlan' parameters: • ipsec-security – Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default. • gw [<IP>|<HOSTNAME>] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway's numerical IP address or administrator defined hostname.

- `mint link ip [<IPv4>|<IPv6>|<HOST-ALIAS-NAME>] {<1-65535>|adjacency-hold-time <2-600>|cost <1-10000>|hello-interval <1-120>|level [1|2]|ipsec-security {gw [<IP>|<HOST-NAME>]}}`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
link ip [<IPv4>|<IPv6>| <HOST-ALIAS-NAME>]	Creates a MiNT routing link • ip – Creates a MiNT tunnel over UDP/IP or IPv6 Use this keyword to specify the IP address (IPv4 or IPv6) used by peers for inter-operation when supporting the MINT protocol. • <IPv4> – Specify the IPv4 address used by peers. • <IPv6> – Specify the IPv6 address used by peers. • <HOST-ALIAS-NAME> – Specify the host alias identifying the MiNT tunnel peer's address. The host alias should existing and configured.
<1-65535>	Select the peer UDP port from 1 - 65535.
adjacency-hold-time <2-600>	Optional. Specifies the adjacency lifetime after hello packets cease • <2-600> – Specify a value from 2 - 600 seconds. The default is 46 seconds.
cost <1-100000>	Optional. Specifies the link cost in arbitrary units • <1-100000> – Specify a value from 1 - 100000. The default is 100.
hello-interval <1-120>	Optional. Specifies the interval, in seconds, between successive hello packets <1-120> – Specify a value from 1 - 120. The default is 15 seconds.
level [1|2]	Optional. Specifies the routing levels for this routing link. The options are: • 1 – Configures local routing • 2 – Configures inter-site routing
ipsec-security {gw [<IP>| <HOST-NAME>]}	Optional. Enables IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default. • gw [<IP>|<HOSTNAME>] – Optional. Configures the IPSec secure gateway. When enabling IPSec, you can optionally specify the IPSec secure gateway's numerical IP address or administrator defined hostname.

- `mint mlcp [ip|ipv6|vlan]`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
mlcp [ip|ipv6|vlan]	Configures the MLCP using the IP address or VLAN. MLCP is used to create a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a wireless controller or service platform, it can be another access point with a path to the wireless controller or service platform. • vlan – Enables MLCP over layer 2 (VLAN) links • ip – Enables MLCP over layer 3 (UDP/IP) links. When enabled, allows adoption over IPv4 address. • ipv6 – Enables MLCP over layer 3 (UDP/IPv6) links. When enabled, allows adoption over IPv6 address.

- `mint rate-limit level2 [link [ip [<IPv4>|<IPv6>] <1-65535>|vlan <1-4094>]| mlcp [ip|ipv6|vlan]] rate <50-1000000> max-burst-size <2-1024> {red-threshold [background|best-effort|video|voice] <0-100>}`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
mint rate-limit level2	Applies rate limits on extended VLAN traffic Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices, or malicious software. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network, and also provides differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform or access point are applied. You can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream).
link [ip <IPv4/IPv6> <1-65535>| vlan <1-4094>]	Configures rate limit parameters applicable for all statically configured MiNT links on level2. Select the link-type as 'IP' or 'VLAN'. • ip <IPv4/IPv6> – Configures rate limits for MiNT link traffic over UDP/IP • <IPv4/IPv6> – Specify the MiNT peer's IPv4 or IPV6 address in the A.B.C.D and X:X::X:X formats respectively. • <1-65535> – Configures the virtual port used for rate limiting traffic. Specify the UDP port from 1 - 65535. • vlan <1-4094 – Configures rate limits for MiNT link traffic on specified VLAN • <1-4094> – Specify the VLAN ID from 1 - 4094.
mlcp [ip|ipv6|vlan]	Configures rate limit parameters applicable for MLCP MLCP creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be an access point with a path to the controller or service platform. • ip – Configures rate-limits for MLCP over UDP/IPv4 links • ipv6 – Configures rate-limits for MLCP over UDP/IPv6 links • vlan – Configures rate-limits for MLCP over VLAN links

rate <50-1000000>	Configures the rate limit from 50 - 1000000 Kbps This limit constitutes a threshold for the maximum number of packets transmitted or received (from all access categories). Traffic exceeding the defined rate is dropped and a log message is generated. The default setting is 5000 Kbps.
max-burst-size <2-1024>	Configures the maximum burst size from 0 - 1024 Kbytes Smaller the burst size, lesser is the probability of the upstream packet transmission resulting in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 Kbytes.
red-threshold [background|best-effort|video|voice] <0-100>	Optional. Configures the *random early detection* (RED) threshold (as a percentage) for the following traffic types: • background – Configures the RED threshold for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%. • best-effort – Configures the RED threshold for low priority best-effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%. • video – Configures the RED threshold for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%. • voice – Configures the RED threshold for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%. • <0-100> – After selecting the traffic type, specify the RED threshold from 0 - 100%.

- `mint spf-latency <0-60>`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
spf-latency <0-60>	Specifies the latency of SPF routing recalculation This option allows you to set the *latency of routing recalculation* option (within the *Shortest Path First* (SPF) field). This option is disabled by default. • <0-60> – Specify the latency from 0 - 60 seconds.

- `mint tunnel-across-extended-vlan`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
tunnel-across-extended-vlan	Enables tunneling of MiNT protocol packets across an extended VLAN. This setting is disabled by default.

- `mint tunnel-controller-load-balancing level1`

mint	Configures MiNT protocol parameters required for MiNT link creation and adoption
tunnel-controller-load-balancing level1	Enables load balancing of MiNT extended VLAN traffic across tunnels • level1 – Enables balancing of load of a tunnel wireless controller or service platform over VLAN links

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#mint level 1 area-id 88

rfs6000-37FABE(config-profile-default-rfs6000)#mint link ip 1.2.3.4 level 2

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4 level 2
 mint level 1 area-id 88
 bridge vlan 1
--More--
rfs7000-37FABE(config-profile-default-rfs6000)#

nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#show context
ap7522 84-24-8D-1B-B9-0C
 use profile default-ap7522
 use rf-domain default
 hostname ap7522-1BB90C
 no staging-config-learnt
nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)

nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#mint inter-tunnel-bridging

nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#show context
ap7522 84-24-8D-1B-B9-0C
 use profile default-ap7522
 use rf-domain default
 hostname ap7522-1BB90C
 no staging-config-learnt
 mint inter-tunnel-bridging
nx9500-6C8809(config-device-84-24-8D-1B-B9-0C)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.56 misconfiguration-recovery-time

Profile Config Commands

Verifies connectivity after a configuration is received

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
misconfiguration-recovery-time [0|<60-300>]
```

Parameters

- `misconfiguration-recovery-time [0|<60-300>]`

<60-300>	Sets the recovery time from 60 - 300 seconds (default is 180 seconds)
0	Disables recovery from misconfiguration

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#misconfiguration-recovery-time 65

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ..............................................
  qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 misconfiguration-recovery-time 65
 service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Reverts to default (180 seconds)

7.1.57 neighbor-inactivity-timeout

Profile Config Commands

Configures neighbor inactivity timeout

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
neighbor-inactivity-timeout <1-1000>
```

Parameters

- `neighbor-inactivity-timeout <1-1000>`

<1-1000>	Sets neighbor inactivity timeout • <1-1000> – Specify a value from 1 - 1000 seconds. The default is 30 seconds.

Example

```
rfs6000-37FABE(config-profile-default)#neighbor-inactivity-timeout 500

rfs6000-37FABE(config-profile-default-rfs7000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 neighbor-inactivity-timeout 500
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

7.1.58 neighbor-info-interval

Profile Config Commands

Configures the neighbor information exchange interval

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
neighbor-info-interval <1-100>
```

Parameters

- `neighbor-info-interval <1-100>`

<1-100>	Sets interval from 1 - 100 seconds. The default is 10 seconds.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#neighbor-info-interval 6

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

7.1.59 no

Profile Config Commands

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [adopter-auto-provisioning-policy-lookup|adoption|alias||application-
policy|area|arp|auto-learn|autogen-uniqueid|autoinstall|bluetooth-detection|
bridge|cdp|cluster|configuration-persistence|controller|critical-resource|
crypto|database-backup|device-upgrade|diag|dot1x|dpi|dscp-mapping|eguest-
server|email-notification|environmental-sensor|events|export|file-sync|
floor|gre|http-analyze|interface|ip|ipv6|lacp|l2tpv3|l3e-lite-table|led|
led-timeout|legacy-auto-downgrade|legacy-auto-update|lldp|load-balancing|
logging|mac-address-table|mac-auth|management-server|memory-profile|
meshpoint-device|meshpoint-monitor-interval|min-misconfiguration-recovery-time|
mint|misconfiguration-recovery-time|noc|ntp|otls|offline-duration|power-
config|preferred-controller-group|preferred-tunnel-controller|radius|raid|
rf-domain-manager|router|spanning-tree|traffic-class-mapping|traffic-shape|
trustpoint|tunnel-controller|use|virtual-controller|vrrp|vrrp-state-check|zone|
wep-shared-key-auth|service]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts this profile's settings based on the parameters passed

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
rfs6000-81742D(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface me1
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface ge6
 interface ge7
```

```
 interface ge8
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 adopter-auto-provisioning-policy-lookup
 router ospf
 router bgp
 adoption start-delay min 10 max 30
rfs6000-81742D(config-profile-default-rfs6000)#

rfs6000-81742D(config-profile-default-rfs6000)#no adopter-auto-provisioning-
policy-lookup
rfs6000-81742D(config-profile-default-rfs6000)#no adoption start-delay

rfs6000-81742D(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
 interface me1
 interface up1
 interface ge1
 interface ge2
 interface ge3
 interface ge4
 interface ge5
 interface ge6
 interface ge7
 interface ge8
 interface wwan1
 interface pppoe1
 use firewall-policy default
 logging on
 service pm sys-restart
 router ospf
 router bgp
rfs6000-81742D(config-profile-default-rfs6000)#
```

7.1.60 noc

Profile Config Commands

Configures *Network Operations Center* (NOC) statistics update interval. This is the interval at which statistical updates are sent by the RF Domain manager to its adopting controller (the NOC controller).

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
noc update-interval [<5-3600>|auto]
```

Parameters

- `noc update-interval [<5-3600>|auto]`

noc update-interval [<5-3600>|auto]	Configures NOC statistics update interval • <5-3600> – Specify the update interval from 5 - 3600 seconds. • auto – The NOC statistics update interval is automatically adjusted by the wireless controller or service platform based on load. This option is enabled by default.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#noc update-interval 25

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 ................................................
 interface pppoe1
 use firewall-policy default
 misconfiguration-recovery-time 65
 noc update-interval 25
 service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Resets NOC related parameters

7.1.61 nsight

Profile Config Commands

Configures NSight database related parameters. Use this command to configure the data-update periodicity, number of applications posted to the NSight server for a wireless client, and the duration for which data is stored in the NSight database's buckets. These parameters impact the amount of data stored in the NSight DB and interval at which data is aggregated and expired within the NSight DB. For more information on data aggregation and expiration, see *(Data Aggregation and Expiration)*.

Configure these parameters in the NSight server's profile configuration mode. These parameters are also configurable on the NSight server's device configuration mode.

Supported in the following platforms:

- Service Platforms — NX9500, NX9510, NX9600, VX9000

Syntax

```
nsight database [statistics|summary]

nsight database statistics [avc-update-interval|max-apps-per-client|max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata|max-ssl-visits-metadata|update-interval|wireless-clients-update-interval]

nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-interval] [120|30|300|60|600]

nsight database statistics max-apps-per-client <1-1000>

nsight database statistics [max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata|max-ssl-visits-metadata] <1-1000>

nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>
```

Parameters

```
• nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-interval] [120|30|300|60|600]
```

nsight database statistics	Configures NSight database statistics related parameters
avc-update-interval	Configures the interval, in seconds, at which *Application Visibility and Control* (AVC) statistics is updated to the NSight database. This interval represents the rate at which AVC-related data is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see *(Data Aggregation and Expiration)*. When configured, RF Domain managers posting AVC-related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the *avc-update-interval* configured here.
update-interval	Configures the interval, in seconds, at which data is updated to the NSIght server. This interval represents the rate at which data (excluding AVC and wireless-clients related statistics) is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see *(Data Aggregation and Expiration)*. Contd...

contd..	When configured, RF Domain managers posting data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the *update-interval* configured here. **Note:** Use the '*avc-update-interval*' and '*wireless-clients-update-interval*' keywords to configure update interval for *AVC-related* and *wireless-clients* related information respectively.
wireless-clients-update-interval	Configures the interval, in seconds, at which wireless-client statistics is updated to the NSIght server. This interval represents the rate at which wireless-clients related statistics is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see *(Data Aggregation and Expiration)*. When configured, RF Domain managers posting wireless-client related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the *wireless-clients-update-interval* configured here.
[120|30|300|60|600]	The following keywords are common to all of the above parameters: • 120 – Sets the data-update periodicity as 120 seconds (2 minutes) • 30 – Sets the data-update periodicity as 30 seconds • 300 – Sets the data-update periodicity as 300 seconds (5 minutes). This is the default setting for the *'avc-update-interval'* and '*wireless-clients-update-interval*' parameters. • 60 – Sets the data-update periodicity as 60 seconds (1 minute). This is the default setting for the '*update-interval*' parameter. • 600 – Sets the data-update periodicity as 600 seconds (10 minutes)

- `nsight database statistics max-apps-per-client <1-1000>`

nsight database statistics	Configures NSight database statistics related parameters
max-apps-per-client	Configures the maximum number of applications per wireless-client to be posted to the NSight server within the configured data-update interval. This information is included in the AVC statistics posted by RF Domain managers to the NSight server.
<1-1000>	Specify the number of applications posted from 1 - 1000. The default is 10 applications per wireless client.

- `nsight database statistics [max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata|max-ssl-visits-metadata] <1-1000>`

nsight database statistics	Configures NSight database statistics related parameters
[max-http-usage-metadata|max-http-visits-metadata|max-ssl-usage-metadata| max-ssl-visits-metadata]	Configures the number of HTTP and/or SSL metadata posted within an update interval • max-http-usage-metadata – Configures the NSight database maximum http-metadata by usage (rx+tx) to be posted in an update-interval • max-http-visits-metadata – Configures the NSight database's maximum http-metadata by the number of visits to be posted within an update-interval • max-ssl-usage-metadata – Configures the NSight database maximum ssl-metadata by usage (rx+tx) to be posted in an update-interval Contd...

contd...	• max-ssl-visits-metadata – Configures the NSight database's maximum ssl-metadata by the number of visits to be posted within an update-interval The following keyword is common to all of the above mentioned metadata options: • <1-1000> – Specify a value from 1 - 1000. The default is 10 metadata for each.

• `nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>`

nsight database summary	Configures the NSight database's per-bucket data storage duration
duration <1-24> <1-168> <1-2160> <24-26280>	Configures the duration for which data is stored on a per-bucket basis • <1-24> – Specify the *bucket 1* duration from 1 - 24 hours (i.e. 1 hour to 1 day). The default is 8 hours. • <1-168> – Specify the *bucket 2* duration from 1 - 168 hours (i.e. 1 hour to 7 days). The default is 24 hours. • <1-2160> – Specify the *bucket 3* duration from 1 - 2160 hours (i.e. 1 hour to 90 days). The default is 7 days (168 hours). • <24-26280> – Specify the *bucket 4* duration from 24 - 26280 hours (i.e. 1 day to 3 years). The default is 365 days (1 year). A bucket is a database collection that holds statistical data for each RF Domain within the network. (Note, only those RF Domain's that are using an NSight policy with the NSight server host configured will post data to the NSight server. (For more information, see *use* in the RF Domain configuration mode.) NSight database has four (4) buckets. The data from each bucket is aggregated and pushed to the next bucket once the data storage duration, specified for the bucket, has exceeded. For more information on data aggregation, see *(Data Aggregation and Expiration)*.

Usage Guidelines(Data Aggregation and Expiration)

Data Aggregation:

The NSight functionality, a data analytics tool, analyzes data that is generated periodically by the nodes within the managed wireless LAN. For large WLAN networks, generating significantly large amount of data, storing data forever is neither feasible nor beneficial. Therefore, older statistics are summarized into aggregated (averaged) records. All records, for a fixed time period in past, are summarized into one record by taking an average of them. Although this causes a loss in the data's granularity, average numbers for any given time period is still available.

Statistical data periodically posted by RF Domain managers to the NSight server are stored in buckets (database collections) within the NSight database. There are four buckets in total. These are:

- First bucket (termed as the RAW bucket) - B1
- Second bucket - B2
- Third bucket - B3
- Fourth bucket - B4

On completion of the data storage duration, records from a bucket are aggregated (at a fixed rate) and inserted into the next bucket. The rate at which records are aggregated into the next bucket becomes the next bucket's granularity. For example, the B1 records (that have exceeded the data storage duration configured for B1) are aggregated (at the rate specified) and inserted into B2. Similarly, data from B2 are aggregated into B3, and from B3 to B4. The fixed rate of aggregation (or granularity) AND default storage duration for each bucket is as follows:

- B1: storage duration 8 hours
- B2: granularity 10 minutes / storage duration 24 hours
- B3: granularity 1 hour / storage duration 7 days
- B4: granularity 1 day / storage duration 1 year

Let us consider (with default update-interval settings) the growth of any one of the statistical buckets.

- Since B1's default data storage duration is 8 hours, B1 will hold a maximum of 960 records per RF Domain after 8 hours (updated at the rate of 30 seconds).
- Since B2's granularity is 10 minutes, every 10 minutes 20 records from the B1 will be aggregated into a single record and inserted into B2.
- Since B2's default storage duration is 24 hours, it will contain a maximum of 144 records per RF Domain after 24 hours.
- Since B3's granularity is 1 hour, every hour 6 records from B2 will be aggregated into a single record and inserted into B3.
- Since B3's default storage duration is 7 days, it will contain a maximum of 168 records per RF Domain after 7 days.
- Since B4's granularity is 1 day, every day 24 records from B3 will be aggregated into a single record and inserted into B4.
- Since B4's default storage duration is 365 days, it will contain a maximum of 365 records per RF Domain after 1 year.

Data Expiration:

The expiration of older records (also referred to as purging or deleting of records) occurs along with data aggregation for each bucket.

Let us consider (with default data storage-duration settings) the expiration of data for any one of the statistical buckets.

- As stated earlier, at the end of 8 hours B1 will have 960 records per RF Domain. After a period of 8 hours and 10 minutes, all 960 records are aggregated into 144 records and inserted into B2. To enable B1 to hold exactly 8 hours worth of data, 20 of the oldest records (corresponding to the first 10 minutes) are purged from B1 at the end of 8 hours and 10 minutes. This expiration cycle is triggered every 10 minutes.
- At the end of 24 hours B2 will have 144 records per RF Domain. After a period of 24 hours and 10 minutes, one of the oldest record (corresponding to the first 10 minutes) is purged from B2. This expiration cycle is triggered every 10 minutes to enable B2 to maintain exactly 24 hours worth of data.
- At the end of 7 days B3 will have 168 records per RF Domain. After a period of 7 days and one hour one of the oldest record (corresponding to the first hour) is purged from B3. This expiration cycle is triggered every 1 hour to enable B3 to maintain exactly 7 days worth of data.
- At the end of 365 days B4 will have 365 records per RF Domain. After 365 days, the oldest records (corresponding to the first day) are purged from B4. This expiration cycle is triggered every 1 day to enable B4 to maintain exactly 365 days worth of data.

Example

```
nx9500-6C8809(config-profile-testNX9500)#nsight database statistics
avc-update-interval 120

nx9500-6C8809(config-profile-testNX9500)#nsight database statistics
update-interval 30

nx9500-6C8809(config-profile-testNX9500)#nsight database statistics
wireless-clients-update-interval 600

nx9500-6C8809(config-profile-testNX9500)#nsight database statistics
max-apps-per-client 20

nx9500-6C8809(config-profile-testNX9500)#nsight database summary duration 12 30
200 500

nx9500-6C8809(config-profile-testNX9500)#show context include-factory | include
nsight
 use nsight-policy nsight-noc
 nsight database statistics update-interval 30
 nsight database statistics wireless-clients-update-interval 600
 nsight database summary duration 12 30 200 500
 nsight database statistics avc-update-interval 120
 nsight database statistics max-apps-per-mu 20
nx9500-6C8809(config-profile-testNX9500)#
```

Related Commands

no	Reverts the NSight database related parameters configured to default values

7.1.62 ntp

Profile Config Commands

Configures the *Network Time Protocol* (NTP) server settings

NTP manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Controllers, service platforms, and access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, a controller resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ntp server <PEER-IP/HOSTNAME> {autokey|key|maxpoll|minpoll|prefer|version}

ntp server <PEER-IP/HOSTNAME> {autokey}

ntp server <PEER-IP/HOSTNAME> {maxpoll [1024|2048|4096|8192]}

ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}

ntp server <PEER-IP> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}

ntp server <PEER-IP/HOSTNAME> {prefer version <1-4>|version <1-4> prefer}
```

Parameters

- `ntp server <PEER-IP/HOSTNAME> {autokey} {prefer version <1-4>|version <1-4>}`

ntp server <PEER-IP/ HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
autokey	Optional. Enables automatic configuration of authentication key for the specified NTP server. This option is disabled by default. If not enabled, use the 'key' option to configure an authentication key for the NTP server.

- `ntp server <PEER-IP/HOSTNAME> {maxpoll [1024|2048|4096|8192]}`

ntp server <PEER-IP/ HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
maxpoll [1024|2048|4096| 8192]	Optional. Configures the maximum polling interval. Once set, the specified NTP server is polled no later than the defined interval. Select one of the following options: • 1024 – Configures the maximum polling interval as 1024 seconds. This is the default setting. • 2048 – Configures the maximum polling interval as 2048 seconds • 4096 – Configures the maximum polling interval as 4096 seconds • 8192 – Configures the maximum polling interval as 8192 seconds

- `ntp server <PEER-IP/HOSTNAME> {minpoll [1024|128|256|512|64]}`

ntp server <PEER-IP/ HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
minpoll [1024|128|256|512| 64]	Optional. Configures the minimum polling interval. Once set, the specified NTP server is polled no sooner than the defined interval. Select one of the following options: • 1024 – Configures the minimum polling interval as 1024 seconds • 128 – Configures the minimum polling interval as 128 seconds • 256 – Configures the minimum polling interval as 256 seconds • 512 – Configures the minimum polling interval as 512 seconds • 64 – Configures the minimum polling interval as 64 seconds. This is the default setting.

- `ntp server <PEER-IP/HOSTNAME> {key <1-65534> md5 [0 <WORD>|2<WORD>|<WORD>]}`

ntp server <PEER-IP/ HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME>> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
key <1-65534> md5 [0 <WORD>| 2 <WORD>|<WORD>]	Optional. Defines the authentication key for the specified NTP server. This option is used to configure the key when 'autokey' configuration is not enabled. • <1-65534> – Specify the peer key number. Should not exceed 64 characters in length. • md5 – Sets MD5 authentication • 0 <WORD> – Configures a clear text password • 2 <WORD> – Configures an encrypted password • <WORD> – Sets an authentication key

- `ntp server <PEER-IP/HOSTNAME> {prefer version <1-4>|version <1-4> prefer}`

ntp server <PEER-IP/ HOSTNAME>	Configures NTP server resources that are used to obtain system time • <PEER-IP/HOSTNAME> – Identifies the NTP server resource by its IP address or hostname. Specify the NTP server's IP address or hostname.
prefer version <1-4>	Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default. • version – Optional. Configures the NTP version • <1-4> – Select the NTP version from 1 - 4. If not specified, the default value of '0' is applied, which implies that the NTP server's version is ignored.
version <1-4> prefer	Optional. Configures the version number used by the specified NTP server resource • <1-4> – Select the NTP version from 1 - 4. The default setting is 0. A value of '0' implies that the NTP server's version is ignored. • prefer – Optional. Designates the specified NTP server as a preferred NTP resource. This setting is disabled by default. The NTP version number specified using the 'version <1-4>' keyword is applied to this preferred NTP resource.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#ntp server 172.16.10.10 version 1
prefer

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
.............................................

 interface pppoe1
 use firewall-policy default
 ntp server 172.16.10.10 prefer version 1
 misconfiguration-recovery-time 65
 noc update-interval 25
 service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.63 otls

Profile Config Commands

Enables support for *OmniTrail Location Server* (OTLS) beacon identification

OmniTrail (offered by OmniTrail technologies) is a Wi-Fi based locationing protocol used in positioning and tracking location solutions. Access points supporting OTLS beacon identification lock their radios to scan channels for beacons with OTLS tags. Beacons received by the access point are matched for the OTLS signature, and in case of a match, the beacons are forwarded to the OTLS server as UDP payload.

Use this command to configure OTLS server details on the AP and enable OTLS data forwarding. Alternately, OTLS parameters can be configured in the AP's profile on the controller or service platform, and pushed to adopted access points. When configured, APs establish connection with the OTLS server and forward OTLS locationing feeds to the server.

Supported in the following platforms:

- Access Points — AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8432, AP8533

Syntax

```
otls [apid|control-port|data-port|forward|server-ip]

otls apid <WORD>

otls control-port <0-65535>

otls data-port [2.4GHz|5GHz] <0-65535>

otls forward [2.4GHz|5GHz] [disable|enable]

otls server-ip <OTLS-SERVER-IP>
```

Parameters

- `otls apid <WORD>`

otls apid <WORD>	Configures a unique identification for the OTLS-enabled access point. The access point *identifier* (APID) enables the OTLS server to identify the AP forwarding the OTLS tag. • <WORD> – Specify an ID for the AP. To ensure that OTLS-enabled APs have unique OTLS ID, it is recommended that the APID is configured in the device context of each AP.

- `otls control-port <0-65535>`

otls control-port <0-65535>	Configures the port used by the AP to establish and maintain connection with the OTLS server • <0-65535> – Specify the control port from 0 - 655635.

- `otls data-port [2.4GHz|5GHz] <0-65535>`

otls data-port [2.4GHz|5GHz] <0-65535>	Configures the port used by the AP to forward OTLS beacons to the OTLS server. However, OTLS data forwarding has to be enabled on the APs. Use the *otls > forward > [2.4GHz|5GHz] > [disable|enable]* command to enable data forwarding. • 2.4GHz – Configures the port used to forward OTLS beacons received on the 2.4 GHz band • 5.0GHz – Configures the port used to forward OTLS beacons received on the 5.0 GHz band The following keyword is common to the above parameters: • <0-65535> – Specify a data-forwarding port from 0 - 65535.

- `otls forward [2.4GHz|5GHz] [disable|enable]`

otls forward [2.4GHz|5GHz] [disable|enable]	Enables or disables OTLS tag forwarding • 2.4GHz – Enables or disables forwarding of OTLS beacons received on the 2.4 GHz band • 5GHz – Enables or disables forwarding of OTLS beacons received on the 5.0 GHz band The following keywords are common to the above parameters: • disable – Disables OTLS tag forwarding. By default OTLS beacon forwarding is disabled for both 2.4 GHz and 5.0 GHz bands. • enable – Enables OTLS tag forwarding

- `otls server-ip <OTLS-SERVER-IP>`

otls server-ip <OTLS-SERVER-IP>	Configures the OTLS server's IP address • <OTLS-SERVER-IP> – Specify the OTLS server's IP address.

Example

```
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls apid 112233
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls forward 2.4GHz enable
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls forward 5GHz enable
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls control-port 8890
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls data-port 2.4GHz 8888
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls data-port 5GHz 8889
ap8533-84A224(config-device-84-24-8D-84-A2-24)#otls server-ip 192.168.13.10

ap8533-84A224(config-device-84-24-8D-84-A2-24)#show context include-factory |
include otls
 otls forward 5GHz enable
 otls forward 2.4GHz enable
 otls server-ip 192.168.13.10
 otls control-port 8890
 otls data-port 2.4GHz 8888
 otls data-port 5GHz 8889
 otls apid 112233
ap8533-84A224(config-device-84-24-8D-84-A2-24)
```

The following example displays OTLS parameters configured on an AP8533 profile:

```
nx9500-6C8809(config-profile-testAP8533)#show context include-factory | include
otls
 otls forward 5GHz enable
 otls forward 2.4GHz enable
 otls server-ip 192.168.13.10
 otls control-port 8890
 otls data-port 2.4GHz 8888
 otls data-port 5GHz 8889
 otls apid 12345
nx9500-6C8809(config-profile-testAP8533)#
```

Related Commands

no	Removes the OTLS-related parameters configured on an AP or on an AP's profile

7.1.64 offline-duration

Profile Config Commands

Sets the duration, in minutes, for which a device remains unadopted before it generates offline event

This command is also supported on the device configuration mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
offline-duration <5-43200>
```

Parameters

- `offline-duration <5-43200>`

offline-duration <5-43200>	Specify a value from 5 - 43200 minutes. The default is 10 minutes.

Example

```
rfs4000-229D58(config-profile-test)#offline-duration 200

rfs4000-229D58(config-profile-test)#show context
profile rfs4000 test
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 ..............................................................
 interface wwan1
 interface pppoe1
 use firewall-policy default
 service pm sys-restart
 router ospf
 offline-duration 200
rfs4000-229D58(config-profile-test)#
```

Related Commands

no	Resets the offline-duration to default (10 minutes)

7.1.65 power-config

Profile Config Commands

Configures the power option mode. Use this command in the profile configuration mode to configure the transmit output power of access point radios. This command is also available in the device-config mode.

Single radio model access points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models. When an access point is powered on for the first time, the system determines the power budget available to the access point. If 802.3af is selected, the access point assumes 12.95 watts is available. If the mode is changed, the access point requires a reset to implement the change. If 802.3at is selected, the access point assumes 23 - 26 watts is available.

NOTE: Single radio model access points (AP6511 and AP6521) always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models.

The access point has to be restarted for power management changes to take effect.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
power-config [af-option|at-option|mode]

power-config [af-option|at-option] [range|throughput]

power-config mode [auto|3af]
```

Parameters

- `power-config [af-option|at-option] [range|throughput]`

power-config	Configures the power option mode
af-option [range|throughput]	Configures the 802.3.af power mode option. The options are: • range – Configures the af power range mode. This mode provides higher power but fewer transmission (tx) chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. • throughput – Configures the af power throughput mode. This mode provides lower power but has more tx chains. This is the default setting. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.

at-option [range|throughput]	Configures the 802.3 at power mode option. The options are: • range – Configures the at power range mode. This mode provides higher power but fewer tx chains. Select range when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. • throughput – Configures the at power throughput mode. This mode provides lower power but has more tx chains. This is the default setting. Select throughput to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where transmission range is secondary to broadcast/multicast transmission performance.

- `power-config mode [auto|3af]`

power-config	Configures the power option mode
mode [auto|3af]	Configures the AP power mode • 3af – Forces an AP to power up in the 802.3af power mode • auto – Sets the detection auto mode (default setting) The automatic power-config mode enables an access point to automatically determine the best power configuration based on the available power budget.

Example

```
nx9500-6C8809(config-profile-testAP7161)#power-config mode 3af

nx9500-6C8809(config-profile-testAP7161)#power-config af-option range

nx9500-6C8809(config-profile-testAP7161)#show context
profile ap71xx testAP7161
 no autoinstall configuration
 no autoinstall firmware
 power-config mode 3af
 power-config af-option range
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 --More--
nx9500-6C8809(config-profile-testAP7161)#
```

Related Commands

no	Reverts the power mode setting on this profile to default

7.1.66 preferred-controller-group

Profile Config Commands

Specifies the controller group preferred for adoption

At adoption, an access point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller or service platform for adoption. After selecting the controller or service platform, the access point associates with it and optionally obtains an image upgrade and configuration. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Use this command to specify the controller or service platform preferred for adoption. Once configured, the access point adopts to the specified preferred controller or service platform.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533

Syntax

```
preferred-controller-group <WORD>
```

Parameters

- `preferred-controller-group <WORD>`

<WORD>	Specify the name of the controller (wireless controller or service platform) group preferred for adoption. Devices using this profile are added, on adoption, to the controller group specified here.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#preferred-controller-group
testGroup

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
.....................................................
 qos trust 802.1p
 interface pppoe1
 use firewall-policy default
 ntp server 172.16.10.10 prefer version 1
 preferred-controller-group testGroup
 misconfiguration-recovery-time 65
 noc update-interval 25
 service pm sys-restart
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Removes the preferred controller group configuration

7.1.67 preferred-tunnel-controller

Profile Config Commands

Configures the tunnel controller's name preferred for tunneling extended VLAN traffic. Devices using this profile will prefer to route their extended VLAN traffic through the specified tunnel controller (wireless controller or service platform).

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
preferred-tunnel-controller <NAME>
```

Parameters

- `preferred-tunnel-controller <NAME>`

preferred-tunnel-controller <NAME>	Configures the preferred tunnel name

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#preferred-tunnel-controller
testtunnel
```

Related Commands

no	Removes the preferred tunnel configuration

7.1.68 radius

Profile Config Commands

Configures device level RADIUS authentication parameters

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
radius [nas-identifier|nas-port-id] <WORD>
```

Parameters

- `radius [nas-identifier|nas-port-id] <WORD>`

radius	Configures RADIUS authentication parameters
nas-identifier <WORD>	Specifies the RADIUS *Network Access Server* (NAS) identifier attribute used by this device • <WORD> – Specifies the NAS identifier
nas-port-id <WORD>	Specifies the RADIUS NAS port ID attribute used by this device • <WORD> – Specifies the NAS port ID

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#radius nas-port-id 1

rfs6000-37FABE(config-profile-default-rfs6000)#radius nas-identifier test

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 radius nas-identifier test
 radius nas-port-id 1
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.69 rf-domain-manager

Profile Config Commands

Configures the RF Domain manager election criteria

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
rf-domain-manager [capable|priority <1-255>]
```

Parameters

- `rf-domain-manager [capable|priority <1-255>]`

rf-domain-manager	Configures the RF Domain manager election criteria
capable	Enables devices using this profile capable of being elected as the RF Domain manager. The RF Domain manager stores and provisions configuration and firmware images for other members of the RF Domain. It also updates state changes, if any, to RF Domain members. This option is enabled by default.
priority <1-255>	Assigns a priority value for devices using this profile in the RF Domain manager election process. The higher the number set, higher is the device's priority in the RF Domain manager election process. • <1-255> – Select a priority value from 1 - 255.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#rf-domain-manager priority 9

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 ..........................................
 rf-domain-manager priority 9
 preferred-controller-group testGroup
 misconfiguration-recovery-time 65
 noc update-interval 25
 service pm sys-restart
 preferred-tunnel-controller testtunnel
 router ospf
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.70 router

Profile Config Commands

Enables dynamic routing (BGP and/or OSPF) and enters the routing protocol configuration mode

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

NOTE: BGP is supported only on RFS4000, RFS6000, NX75XX, and NX9500 model controllers and service platforms.

The NX9500 and NX9510 service platforms do not support OSPF routing.

The access points only support OSPF routing.

Syntax

```
router [bgp|ospf]
```

Parameters

- `router [bgp|ospf]`

router	Enables dynamic routing and enters the routing protocol configuration mode
bgp	Enables BGP dynamic routing and configures relevant settings BGP is an inter-ISP routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP uses TCP as its transport protocol, eliminating the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. Routing information exchanged through BGP supports destination based forwarding only. It assumes a router forwards packets based on the destination address carried in the IP header of the packet. An AS is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. For more information on dynamic BGP routing configurations, see *BORDER GATEWAY PROTOCOL*.
ospf	Enables OSPF dynamic routing and configures relevant settings. Changes configuration mode to router mode OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. For more information on dynamic OSPF routing configurations, see *ROUTER-MODE COMMANDS*.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#router ospf

rfs6000-37FABE(config-profile default-rfs6000-router-ospf)#?
Router OSPF Mode commands:
  area                  OSPF area
  auto-cost             OSPF auto-cost
  default-information   Distribution of default information
  ip                    Internet Protocol (IP)
  network               OSPF network
  no                    Negate a command or set its defaults
  ospf                  Ospf
  passive               Make OSPF Interface as passive
  redistribute          Route types redistributed by OSPF
  route-limit           Limit for number of routes handled OSPF process
  router-id             Router ID

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-profile default-rfs6000-router-ospf)#
```

Related Commands

no	Disables OSPF settings

7.1.71 spanning-tree

Profile Config Commands

Enables spanning tree commands. Use these commands to configure the errdisable, multiple spanning tree and portfast settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
spanning-tree [errdisable|mst|portfast]

spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]

spanning-tree mst [<0-15>|cisco-interoperability|enable|forward-time|hello-
time|instance|max-age|max-hops|region|revision]

spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability
[enable|disable]|enable|forward-time <4-30>|hello-time <1-10>|instance <1-15>|
max-age <6-40>|max-hops <7-127>|region <LINE>|revision <0-255>]

spanning-tree portfast [bpdufilter|bpduguard] default
```

Parameters

- `spanning-tree errdisable recovery [cause bpduguard|interval <10-1000000>]`

spanning-tree	Configures spanning-tree related parameters
errdisable	Disables or shuts down ports where traffic is looping, or ports with traffic in one direction
recovery	Enables the timeout mechanism for a port to be recovered. This option is disabled by default.
cause bpduguard	Specifies the reason for errdisable • bpduguard – Recovers from errdisable due to bpduguard
interval <10-1000000>	Specifies the interval after which a port is enabled • <10-1000000> – Specify a value from 10 - 1000000 seconds. The default is 300 seconds.

- `spanning-tree mst [<0-15> priority <0-61440>|cisco-interoperability [enable|disable]|enable|forward-time <4-30>|hello-time <1-10>|instance <1-15>| max-age <6-40>|max-hops <7-127>|region <LINE>|revision <0-255>]`

spanning-tree	Configures spanning-tree related parameters
mst	Configures *Multiple Spanning Tree* (MST) commands The MSTP provides an extension to STP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

<0-15> priority <0-61440>	Specifies the number of instances required to configure MST. Select a value from 0 - 15. • priority – Sets the bridge priority to the specified value. This value is used to determine the root bridge. Use the no parameter with this command to restore the default bridge priority value. • <0-61440> – Sets the bridge priority in increments (Lower priority indicates greater likelihood of becoming root)
cisco interoperability [enable|disable]	Enables CISCO interoperability Enables interoperability with CISCO's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
enable	Enables MST protocol
forward-time <4-30>	Specifies the forwarding delay time in seconds • <4-30> – Specify a value from 4 - 30 seconds. The default is 15 seconds.
hello-time <1-10>	Specifies the hello BDPU interval in seconds • <1-10> – Specify a value from 1 - 10 seconds. The default is 2 seconds.
instance <1-15>	Defines the instance ID to which the VLAN is associated • <1-15> – Specify an instance ID from 1 - 10.
max-age <6-40>	Defines the maximum time to listen for the root bridge • <6-40> – Specify a value from 4 - 60 seconds. The default is 20 seconds.
max-hops <7-127>	Defines the maximum hops when BPDU is valid • <7-127> – Specify a value from 7 - 127. The default is 20.
region <LINE>	Specifies the MST region • <LINE> – Specify the region name.
revision <0-255>	Sets the MST bridge revision number. This enables the retrieval of configuration information. • <0-255> – Specify a value from 0 - 255. This default is 0.

- `spanning-tree portfast [bpdufilter|bpduguard] default`

spanning-tree	Configures spanning-tree related parameters
portfast [bpdufilter| bpduguard] default	Enables PortFast on a bridge • bpdufilter default – Sets the BPDU filter for the port. The BPDU filter is disabled by default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures that PortFast enabled ports do not transmit or receive BPDUs. • bpduguard default – Guards PortFast ports against BPDU receive. The BPDU guard is disabled by default. Enabling the BPDU guard means this port will shutdown on receiving a BPDU. • default – Enables the BPDU filter and/or BPDU guard on PortFast enabled ports by default

Usage Guidelines

If a bridge does not hear BPDUs from the root bridge within the specified interval, assume the network has changed and recomputed the spanning-tree topology.

Generally, spanning tree configuration settings in the config mode define the configuration for bridge and bridge instances.

MSTP is based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.

Wireless Controllers or service platforms with the same instance, VLAN mapping, revision number and region names define a unique region. Wireless Controllers or service platforms in the same region exchange BPDUs with instance record information within.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#spanning-tree errdisable recovery
cause bpduguard

rfs6000-37FABE(config-profile-default-rfs6000)#spanning-tree mst 2 priority 4096

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 radius nas-identifier test
 radius nas-port-id 1
 neighbor-info-interval 6
 neighbor-inactivity-timeout 500
 spanning-tree mst 2 priority 4096
 spanning-tree errdisable recovery cause bpduguard
 autoinstall configuration
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables or reverts settings to their default

7.1.72 traffic-class-mapping

Profile Config Commands

Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority. This mapping is required to provide priority of service to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic. Devices use the traffic class field in the IPv6 header to set this priority. This command allows you to assign a priority for different IPv6 traffic types.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>
```

Parameters

- `traffic-class-mapping <IPv6-TRAFFIC-CLASS-VALUE> priority <0-7>`

traffic-class-mapping	Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority
<IPv6-TRAFFIC-CLASS-VALUE>	Specify the traffic class value of incoming IPv6 untagged packet(s) (could be a single value or a list. For example, 10-20, 25, 30-35). This is the DSCP 6-bit parameter in the header of every IP packet used for packet classification.
priority <0-7>	Specify the 802.1p priority to map with the traffic-class value specified in the previous step • <0-7> – Specify a value from 0 - 7. The 802.1p priority is a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are: • 0 – Best Effort • 1 – Background • 2 – Spare • 3 – Excellent Effort • 4 – Controlled Load • 5 – Video • 6 – Voice • 7 – Network Control

Example

```
rfs4000-229D58(config-profile-TestRFS4000)#traffic-class-mapping 25 priority 2

rfs4000-229D58(config-profile-TestRFS4000)#show context
profile rfs4000 TestRFS4000
 traffic-class-mapping 25 priority 2
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto remote-vpn-client
-More-
rfs4000-229D58(config-profile-TestRFS4000)#
```

Related Commands

no	Removes mapping between IPv6 traffic class value (of incoming IPv6 untagged packets) and 802.1p priority

7.1.73 traffic-shape

Profile Config Commands

Enables traffic shaping and configures traffic shaping parameters. This command is applicable to both the profile and device configuration modes.

Traffic shaping is a means of regulating data transfers and ensuring a specific level of performance within a network. Traffic shaping does the following:

- Controls flow of packets based on their priority value. Prioritized traffic streams are given priority over less important traffic.
- Controls traffic on an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms to applied policies
- Shapes traffic to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Use this option to apply traffic shaping to specific applications or application categories. Note, in scenarios where a traffic class is matched against an application, application-category, and ACL rule, the application rule will be applied first, followed by the application-category, and finally the ACL. Further, using traffic shaping, an application takes precedence over an application category.

To enable traffic shaping, configure QoS values on the basis of which priority of service is provided to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic. For configuring IPv6 traffic class mappings, see *traffic-class-mapping*. And for configuring DSCP traffic class mappings, see *dscp-mapping*.

Supported in the following platforms:

- Access Points — AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530

Syntax

```
traffic-shape [activation-criteria|app-category|application|class|enable|
priority-map|total-bandwidth]

traffic-shape activation-criteria [always|cluster-master|rf-domain-manager|vrrp-
master <1-255>]

traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>

traffic-shape application <APPLICATION-NAME> class <1-4>

traffic-shape class <1-4> [max-buffers|max-latency|rate]

traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>|red-percent <1-
100>}

traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]

traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]|total-bandwidth-percent <1-
100>]
```

NOTE: The available range for the 'rate' field will vary depending on the unit selected. It is 250 - 250000 for Kbps and 1 - 250 for Mbps.

```
traffic-shape priority-map <0-7>

traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]
```

NOTE: The available range for the 'total-bandwidth' field will vary depending on the unit selected. It is 250 - 1000000 for Kbps and 1 - 1000 for Mbps.

```
traffic-shape enable
```

Parameters

- `traffic-shape activation-criteria [always|cluster-master|rf-domain-manager| vrrp-master <1-255>]`

traffic-shape activation-criteria	Configures traffic-shape activation criteria that determines when the device invokes traffic shaping
always	Always invokes traffic shaping. This is the default setting.
cluster-master	Invokes traffic shaping when the device is the cluster master. The solitary cluster master (elected using a priority assignment scheme) is a cluster member that provides management configuration and Smart RF data to other members within the cluster. Cluster requests go through the elected master before dissemination to other cluster members.
rf-domain-manager	Invokes traffic shaping when the device is the RF Domain manager. The RF Domain manager is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain.
vrrp-master <1-255>	Invokes traffic shaping when the device is the VRRP master. As the VRRP master, the device responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. • <1-255> – Specify the VRRP group ID from 1 - 255.

- `traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>`

traffic-shape app-category <APP-CATEGORY-NAME> class <1-4>	Configures an application category to traffic-class mapping. Use this option to apply an application category to traffic-shaper class mapping. Naming and categorizing applications that do not fall into existing groups is an additional means of filtering and potentially limiting network airtime to consumptive non required applications negatively impacting network performance. **Note:** app-category <APP-CATEGORY-NAME> – Specify the application category name. To list the available application categories, press [TAB] after entering app-category. Select the required category from the displayed list. Contd..

	• class <1-4> – Map the specified application category to a traffic-shaper class from 1 - 4. Before configuring an application category to class mapping, ensure that the specified classes have been configured. Use the *'class > [max-buffers|max-latency|rate]'* option available with this command to configure a traffic shaper class. For more information, see following parameter tables.

• `traffic-shape application <APPLICATION-NAME> class <1-4>`

traffic-shape app-category <APPLICATION-NAME> class <1-4>	Configures an application to traffic-class mapping. Use this option to apply an application to traffic-shaper class mapping. • app-category <APPLICATION-NAME> – Specify the application name. • class <1-4> – Map the specified application to a traffic-shaper class from 1 - 4. **Note:** Before configuring an application to class mapping, ensure that the specified classes have been configured. Use the *'class > [max-buffers|max-latency|rate]* option available with this command to configure a traffic shaper class. For more information, see following tables.

• `traffic-shape class <1-4> max-buffers <1-400> {red-level <1-400>|red-percent <1-100>}`

traffic-shape class <1-4> max-buffers <1-400>	Configures the queue length limit for different traffic-shaper class • class <1-4> – Specify the traffic-shaper class from 1 - 4. • max-buffers <1-400> – Configures the maximum queue lengths for packets of different priority queues, after which the queue starts to drop packets. • <1-400> – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7. **Note:** For access points the upper queue length limit is 400.
red-level <1-400>	Optional. Performs *Random Early Drop* (RED) when a specified queue length in packets is reached • <1-400> – Configure the queue length limit from 1 - 400 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7. The RED algorithm is a queuing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped. **Note:** For more information on default values, see the Usage Guidelines section in this topic.
red-percent <1-100>	Optional. Performs RED when a specified value, which is a percentage of the max-buffers configured, is reached • <1-100> – Configure the percentage of the maxi-buffers from 1 - 100 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7.

- `traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]`

traffic-shape class <1-4> max-latency <1-1000000> [msec|usec]	Configures the max-latency for different traffic-shaper class. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8. • class <1-4> – Specify the traffic-shaper class from 1 - 4. • max-latency <1-1000000> – Configures the max-latency for packets of different priority queues, after which the queue starts to drop packets. • <1-1000000> – Configure the max-latency from 1 - 100000 for packets of priority queues 0, 1, 2, 3, 4, 5, 6, and 7. • [msec|usec] – Configures the unit for measuring latency as milliseconds (msec) or microseconds (usec). The default setting is msec.

- `traffic-shape class <1-4> rate [<1-250000> [Kbps|Mbps]|total-bandwidth-percent <1-100>]`

traffic-shape class <1-4> rate	Configures traffic rate, in either Kbps, Mbps or percentage, for the different traffic shaper class. Specify rates for different traffic shaper class to control the maximum traffic rate sent or received on an interface. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority. • class <1-4> – Specify the traffic-shaper class from 1 - 4.
<1-250000> [Kbps|Mbps]	Configures the traffic rate, in Kbps, Mbps, for the class specified in the previous step • <1-250000> – Specify the rate from 1 - 250000. • [Kbps|Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Kbps. **Note:** The range varies depending on the unit selected. It is 1 - 250 Mbps, or 250 - 250000 Kbps.
total-bandwidth-percent <1-100>	Configures the traffic rate, as a percentage of the total available bandwidth, for the class specified in the previous first step • <1-100> – Specify the traffic rate from 1 - 100% of the total bandwidth.

- `traffic-shape priority-map <0-7>`

traffic-shape priority-map <0-7>	Configures the traffic-shaper queues, within a class, having different priority values (0, 1, 2, 3, 4, 5, 6, and 7). There are 8 queues (0 - 7), and traffic is queued in each based on the incoming packet's 802.1p 3-bit priority markings. • priority-map <0-7> – Specify the priority from 0 - 7 for priority levels 0, 1, 2, 3, 4, 5, 6, and 7. The IEEE 802.1p standards sets a 3-bit value in the MAC header to indicate prioritization. This 3-bit value provides priority levels ranging from 0 to 7 (i.e., a total of 8 levels), with level 7 representing the highest priority. This permits packets to cluster and form different traffic classes. In case of network congestion, packets with higher priority receive preferential treatment while low priority packets are kept on hold.

- `traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]`

traffic-shape total-bandwidth <1-1000000> [Kbps|Mbps]	Configures the total-bandwidth for traffic shaping • <1-1000000> – Specify the value from 1 - 1000000 Kbps/Mbps. The default value is 10 Mbps. • [Kbps|Mbps] – Configures the unit for measuring bandwidth as Kbps or Mbps. The default setting is Mbps. **Note:** The range varies depending on the unit selected. It is 1 - 1000 Mbps, or 250 - 1000000 Kbps.

- `traffic-shape enable`

traffic-shape enable	Enables traffic shaping using the defined bandwidth, rate and class mappings configured using this command **Note:** Traffic shaping is disabled by default.

Usage Guidelines

Following are the default max-buffers set for the traffic shaper classes:

```
traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20
15 10
traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20
15 10
traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20
15 10
traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23 25 20
15 10
```

Following is the default priority-map settings:

```
traffic-shape priority-map 2 0 1 3 4 5 6 7
```

Example

```
nx9500-6C8809(config-profile-ProfileNX5500)#show context include-factory |
include traffic-shape
 traffic-shape priority-map 2 0 1 3 4 5 6 7
 traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape activation-criteria always
 traffic-shape total-bandwidth 10 Mbps
 no traffic-shape enable
nx9500-6C8809(config-profile-ProfileNX5500)#

nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape enable
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape class 1 rate 250 Mbps
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape application Bing class
1
nx9500-6C8809(config-profile-ProfileNX5500)#traffic-shape total-bandwidth 200
Mbps
```

```
nx9500-6C8809(config-profile-ProfileNX5500)#show context include-factory |
include traffic-shape
 traffic-shape priority-map 2 0 1 3 4 5 6 7
 traffic-shape class 1 rate 250 Mbps
 traffic-shape class 1 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape class 2 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape class 3 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape class 4 max-buffers 35 35 35 30 25 20 15 10 red-level 27 27 27 23
25 20 15 10
 traffic-shape activation-criteria always
 traffic-shape application Bing class 1
 traffic-shape total-bandwidth 200 Mbps
 traffic-shape enable
nx9500-6C8809(config-profile-ProfileNX5500)#
```

Related Commands

no	Removes traffic shaping configuration or reverts them to the default values

7.1.74 trustpoint (profile-config-mode)

Profile Config Commands

Configures the trustpoint assigned for validating a CMP auth Operator

A certificate links identity information with a public key enclosed in the certificate.

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain the CA certificate in its Trusted Root Library so it can trust certificates signed by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

NOTE: Certificates/trustpoints used in this command should be verifiable as existing on the device.

NOTE: For information on configuring trustpoints on a device, see *trustpoint (device-config-mode)*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
trustpoint [cmp-auth-operator|https|radius-ca|radius-server] <TRUSTPOINT-NAME>
```

Parameters

- `trustpoint [cmp-auth-operator|https|radius-ca|radius-server] <TRUSTPOINT-NAME>`

trustpoint	Assigns an existing trustpoint to validate CMP auth operator, client certificates, and RADIUS server certificate
https	Assigns an existing trustpoint to validate HTTPS requests

cmp-auth-operator	Assigns an existing trustpoint to validate CMP auth operator Once validated, CMP is used to obtain and manage digital certificates in a PKI network. Digital certificates link identity information with a public key enclosed within the certificate, and are issued by the CA. Use this command to specify the CMP-assigned trustpoint. When specified, devices send a certificate request to the CMP supported CA server, and download the certificate directly from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.
radius-ca	Assigns an existing trustpoint to validate client certificates in EAP
radius-server	Assigns an existing trustpoint to validate RADIUS server certificate
<TRUSTPOINT-NAME>	The following keyword is common to all of the above parameters: • <TRUSTPOINT-NAME> – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device).

Example

```
nx9500-6C8809(config-profile-testNX9500)#trustpoint cmp-auth-operator test

nx9500-6C8809(config-profile-testNX9500)#show context
profile nx9000 testNX9500
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
.....................................................
 service pm sys-restart
 router bgp
 trustpoint cmp-auth-operator test
nx9500-6C8809(config-profile-testNX9500)#
```

Related Commands

no	Removes trustpoint-related configurations

7.1.75 tunnel-controller

Profile Config Commands

Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
tunnel-controller <NAME>
```

Parameters

- `tunnel-controller <NAME>`

tunnel-controller <NAME>	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name • <NAME> – Specify the name.

Example

```
rfs7000-37FABE(config-profile-default-rfs7000)#tunnel-controller testgroup
```

Related Commands

no	Removes the configured the tunneled WLAN (extended VLAN) wireless controller or service platform's name

7.1.76 use

Profile Config Commands

Associates existing policies with this profile. This command is also applicable to the device configuration mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax Profiles Mode

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-
forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy|
database-client-policy|dhcp-server-policy|dhcpv6-server-policy|
event-system-policy|firewall-policy|global-association-list|guest-management|
ip-access-list|ipv6-access-list|management-policy|radius-server-policy|
role-policy|routing-policy|web-filter-policy] <POLICY-NAME>

use ip/ipv6-access-list <IP/IPv6-ACL-NAME> traffic-shape class <1-4>
```

Syntax Device Mode

```
use [auto-provisioning-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-
forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy|
database-client-policy|database-policy|dhcp-server-policy|dhcpv6-server-policy|
enterprise-ui|event-system-policy|firewall-policy|global-association-list|
guest-management|ip-access-list|ipv6-access-list|license|management-policy|
nsight-policy|profile|radius-server-policy|rf-domain|role-policy|routing-policy|
rtl-server-policy|sensor-policy|web-filter-policy||wips-policy] <POLICY-NAME>
```

NOTE: The following tables contain the 'use' command parameters for the Profile and Device configuration modes.

Parameters Profiles Mode

```
• use [auto-provisioning-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-
forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy|
database-client-policy|dhcp-server-policy|dhcpv6-server-policy|event-system-
policy|firewall-policy|global-association-list|guest-management|ip-access-list|
ipv6-access-list|management-policy|radius-server-policy|role-policy|
routing-policy|web-filter-policy] <POLICY-NAME>
```

use	Associates the specified policies with this profile The specified policies should be existing and configured.
auto-provisioning-policy <POLICY-NAME>	Associates an auto provisioning policy • <POLICY-NAME> – Specify the auto provisioning policy name.

bonjour-gw-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Forwarding policy name (should be existing and configured). For more information on Bonjour GW Forwarding policy, see *bonjour-gw-forwarding-policy*.
bonjour-gw-query-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Query Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).
captive-portal server <CAPTIVE-PORTAL>	Configures access to a specified captive portal with this profile • <CAPTIVE-PORTAL> – Specify the captive portal name.
client-identity-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Associates an existing client identity group with this profile • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name. For more information on the 'client-identity' and 'client-identity-group' commands, see *client-identity* and *client-identity-group*.
crypto-cmp-policy <POLICY-NAME>	Associates an existing crypto *certificate management protocol* (CMP) policy with this profile • <POLICY-NAME> – Specify the CMP policy name. For more information on configuring a crypto CMP policy, see *CRYPTO-CMP-POLICY*.
database-client-policy <POLICY-NAME>	Associates an existing database client policy with a profile • <POLICY-NAME> – Specify the policy name (should be existing and configured). For more information on database client policy, see *database-client-policy*. Applicable only to the VX9000 model virtual machine platform.
dhcp-server-policy <DHCP-POLICY>	Associates a DHCP server policy • <DHCP-POLICY> – Specify the DHCP server policy name.
dhcpv6-server-policy <DHCPv6-POLICY>	Associates a DHCPv6 server policy • <DHCPv6-POLICY> – Specify the DHCPv6 server policy name.
event-system-policy <EVENT-SYSTEM-POLICY>	Associates an event system policy • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.
firewall-policy <FW-POLICY>	Associates a firewall policy • <FW-POLICY> – Specify the firewall policy name.
global-association-list server <GLOBAL-ASSOC-LIST-NAME>	Associates the specified global association list with the controller profile • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name. Once associated, the controller, using this profile, applies this association list to requests received from all adopted APs. For more information on global association list, see *global-association-list*.
guest-management <GUEST-MANAGEMENT-POLICY-NAME>	Associates the specified guest management policy with the controller profile • <GUEST-MANAGEMENT-POLICY-NAME> – Specify the guest management policy name (should be existing and configured).

ip/ipv6-access-list <IP/IPv6-ACL-NAME> traffic-shape class <1-4>	Associates an IP and/or IPv6 ACL with this profile and applies it as a firewall for the selected traffic-shape class • <IP/IPv6-ACL-NAME> – Specify the IP/IPv6 ACL name (should be existing and configured) • traffic-shape class <1-4> – Selects the traffic-shape class to apply the above specified IP/IPv6 ACL • <1-4> – Select the traffic-shape class from 1 - 4.
management-policy <MNGT-POLICY>	Associates a management policy • <MNGT-POLICY> – Specify the management policy name.
radius-server-policy <RADIUS-POLICY>	Associates a device onboard RADIUS policy • <RADIUS-POLICY> – Specify the RADIUS policy name.
role-policy <ROLE-POLICY>	Associates a role policy • <ROLE-POLICY> – Specify the role policy name.
routing-policy <ROUTING-POLICY>	Associates a routing policy • <ROUTING-POLICY> – Specify the routing policy name.
	•
web-filter-policy <POLICY-NAME>	Associates an existing Web Filter policy with a profile or device • <POLICY-NAME> – Specify the policy name.

Parameters Device Mode

```
• use [auto-provisioning-policy|bonjour-gw-forwarding-policy|bonjour-gw-query-
forwarding-policy|captive-portal|client-identity-group|crypto-cmp-policy|
database-client-policy|database-policy|dhcp-server-policy|dhcpv6-server-policy|
enterprise-ui|event-system-policy|firewall-policy|global-association-list|guest-
management|ip-access-list|ipv6-access-list|license|management-policy|nsight-
policy|profile|radius-server-policy|rf-domain|role-policy|routing-policy|rtls-
server-policy|sensor-policy|wips-policy|smart-rf-policy|web-filter-policy]
<POLICY-NAME>
```

use	Associates the following policies with this device:
auto-provisioning-policy <POLICY-NAME>	Associates an auto provisioning policy • <POLICY-NAME> – Specify the auto provisioning policy name.
bonjour-gw-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Forwarding policy name (should be existing and configured). For more information on Bonjour GW Forwarding policy, see *bonjour-gw-forwarding-policy*.
bonjour-gw-query-forwarding-policy <POLICY-NAME>	Uses an existing Bonjour GW Query Forwarding policy with a profile or device • <POLICY-NAME> – Specify the Bonjour GW Query Forwarding policy name (should be existing and configured).
captive-portal server <CAPTIVE-PORTAL>	Configures access to a specified captive portal • <CAPTIVE-PORTAL> – Specify the captive portal name.

client-identity-identity-group <CLIENT-IDENTITY-GROUP-NAME>	Associates an existing client identity group with this device • <CLIENT-IDENTITY-GROUP-NAME> – Specify the client identity group name. For more information on the 'client-identity' and 'client-identity-group' commands, see *client-identity*and *client-identity-group*.
crypto-cmp-policy <POLICY-NAME>	Associates an existing crypto *certificate management protocol* (CMP) policy • <POLICY-NAME> – Specify the CMP policy name. For more information on configuring a crypto CMP policy, see *CRYPTO-CMP-POLICY*.
database-client-policy <POLICY-NAME>	Associates an existing database client policy with a device • <POLICY-NAME> – Specify the policy name (should be existing and configured). For more information on database client policy, see *database-client-policy*. Applicable only to the NX95XX and VX9000 model service platforms.
database-policy <DATABASE-POLICY-NAME>	Associates an existing database policy with this device • <DATABASE-POLICY-NAME> – Specify the database policy name. **Note:** For more information on configuring a database policy, see *database-policy*.
dhcp-server-policy <DHCP-POLICY>	Associates a DHCP server policy • <DHCP-POLICY> – Specify the DHCP server policy name.
dhcpv6-server-policy <DHCPv6-POLICY>	Associates a DHCPv6 server policy • <DHCPv6-POLICY> – Specify the DHCPv6 server policy name.
enterprise-ui	Enables application of the site controller's Enterprise *user interface* (UI) on all management points (controllers and access points) For example, the site controller is NX5500 and a AP7532 is adopted to it. To enable the access point to also use the Enterprise UI: On the AP7532's profile configuration mode execute: *use > enterprise-ui* On adoption and application of this profile, the AP7532 access point resets and reboots using the Enterprise UI. Once using the Enterprise UI, on all subsequent adoptions, the AP does not get reset.
event-system-policy <EVENT-SYSTEM-POLICY>	Associates an event system policy • <EVENT-SYSTEM-POLICY> – Specify the event system policy name.
firewall-policy <FW-POLICY>	Associates a firewall policy • <FW-POLICY> – Specify the firewall policy name.
global-association-list server <GLOBAL-ASSOC-LIST-NAME>	Associates the specified global association list with the device (controller) • <GLOBAL-ASSOC-LIST-NAME> – Specify the global association list name. Once associated, the controller applies this association list to requests received from all adopted APs. For more information on global association list, see *global-association-list*.
guest-management <GUEST-MANAGEMENT-POLICY-NAME>	Associates the specified guest management policy with this device • <GUEST-MANAGEMENT-POLICY-NAME> – Specify the guest management policy name (should be existing and configured).

ip/ipv6-access-list <IP/IPv6-ACL-NAME> traffic-shape class <1-4>	Associates an IP and/or IPv6 ACL with this device and applies it as a firewall for a selected traffic-shape class • <IP/IPv6-ACL-NAME> – Specify the IP/IPv6 ACL name (should be existing and configured) • traffic-shape class <1-4> – Selects the traffic-shape class to apply the above specified IP/IPv6 ACL • <1-4> – Select the traffic-shape class from 1 - 4.
license <WORD>	Associates a Web filtering license with this device • <WORD> – Provide a 256 character maximum license string for the Web filtering feature. Web filtering is used to restrict access to specific resources on the Internet.
management-policy <MNGT-POLICY>	Associates a management policy • <MNGT-POLICY> – Specify the management policy name.
nsight-policy <NSIGHT-POLICY-NAME>	Associates a specified NSight policy with this device • <NSIGHT-POLICY-NAME> – Specify the NSight policy name (should be existing and configured). **Note:** Use this command to associate an NSight policy to a controller to enable it to function as the NSight server. For more information, see *nsight-policy*.
profile <PROFILE-NAME>	Associates a profile with this device • <PROFILE-NAME> – Specify the profile name.
radius-server-policy <RADIUS-POLICY>	Associates a device onboard RADIUS policy • <RADIUS-POLICY> – Specify the RADIUS policy name.
rf-domain <RF-DOMAIN-NAME>	Associates an RF Domain • <RF-DOMAIN-NAME> – Specify the RF Domain name.
role-policy <ROLE-POLICY>	Associates a role policy • <ROLE-POLICY> – Specify the role policy name.
routing-policy <ROUTING-POLICY>	Associates a routing policy • <ROUTING-POLICY> – Specify the routing policy name.
rtl-server-policy <POLICY-NAME>	Associates a *Real TIme Locationing* (RTL) server policy with an access point. When associated, enables the access point to directly send RSSI feeds to the third-party Euclid RTL server • <POLICY-NAME> – Specify the RTL server policy name (should be existing and configured).
sensor-policy <POLICY-NAME>	Associates a sensor policy with an access point or controller. When associated, WiNG controllers and access points function as sensors. • <POLICY-NAME> – Specify the sensor policy name (should be existing and configured).
wips-policy <WIPS-POLICY>	Associates a WIPS policy • <WIPS-POLICY> – Specify the WIPS policy name.
web-filter-policy <POLICY-NAME>	Associates an existing Web Filter policy with a profile or device • <POLICY-NAME> – Specify the policy name.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#use event-system-policy
TestEventSysPolicy

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 mint link ip 1.2.3.4
 mint level 1 area-id 88
 ................................................
 interface ge3
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge4
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface pppoe1
 use event-system-policy TestEventSysPolicy
 use firewall-policy default
 ntp server 172.16.10.10 prefer version 1
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disassociates a specified policy from this profile

7.1.77 vrrp

Profile Config Commands

Configures VRRP group settings

A default gateway is a critical resource for connectivity. However, it is prone to a single point of failure. Thus, redundancy for the default gateway is required. If WAN backhaul is available, and a router failure occurs, then the controller should act as a router and forward traffic on to its WAN link.

Define an external VRRP configuration when router redundancy is required in a network requiring high availability.

Central to VRRP configuration is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router's MAC address
- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.

The nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
vrrp [<1-255>|version]

vrrp <1-255> [delta-priority|description|interface|ip|monitor|preempt|priority|
sync-group|timers]

vrrp <1-255> [delta-priority <1-253>|description <LINE>|ip <IP> {<IP>}|preempt
{delay <1-65535>}|priority <1-254>|sync-group]

vrrp <1-255> interface vlan <1-4094>

vrrp <1-255> monitor [<IF-NAME>|critical-resource|pppoe1|vlan|wwan1]

vrrp <1-255> monitor [<IF-NAME>|pppoe1|vlan <1-4094>|wwan1] {(<IF-NAME>|critical-
resource|pppoe1|vlan|wwan1)}

vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3> <CRM-
NAME4> (action [decrement-priority|increment-priority] {<IF-NAME>|pppoe1|
vlan|wwan1})

vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]
```

```
vrrp version [2|3]
```

Parameters

```
• vrrp <1-255> [delta-priority <1-253>|description <LINE>|vrrp ip <IP> {<IP>}|
preempt {delay <1-65535>}|priority <1-254>|sync-group]
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
delta-priority <1-253>	Configures the priority to decrement (local link monitoring and critical resource monitoring) or increment (critical resource monitoring). When the monitored interface is down, the configured priority decrements by a value defined by the delta-priority option. When monitoring critical resources, the value increments by the delta-priority option. • <1-253> – Specify the delta priority level from 1- 253.
description <LINE>	Configures a text description for the virtual router to further distinguish it from other routers with similar configuration • <LINE> – Provide a description (a string from 1- 64 characters in length)
ip <IP-ADDRESSES>	Identifies the IP address(es) backed by the virtual router. These are IP addresses of Ethernet switches, routers, and security appliances defined as virtual router resources. • <IP-ADDRESSES> – Specify the IP address(es) in the A.B.C.D format. This configuration triggers VRRP operation.
preempt {delay <1-65535>}	Controls whether a high priority backup router preempts a lower priority master. This field determines if a node with higher priority can takeover all virtual IPs from a node with lower priority. This feature is disabled by default. • delay – Optional. Configures the pre-emption delay timer from 1 - 65535 seconds (default is 0 seconds). This option can be used to delay sending out the master advertisement or, in case of monitored link coming up, adjusting the VRRP priority by priority delta.
priority <1-254>	Configures the priority level of the router within a VRRP group. This value determines which node is elected as the Master. Higher values imply higher priority, value 254 has the highest precedence (default is 100).
sync-group	Adds this VRRP group to a synchronized group. To trigger VRRP failover, it is essential all individual groups within a synchronized group have failover. VRRP failover is triggered if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This feature is disabled by default.

```
• vrrp <1-255> interface vlan <1-4094>
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
interface vlan <1-4094>	Enables VRRP on the specified *switch VLAN interface* (SVI) • vlan <1-4094> – Specify the VLAN interface ID from 1 - 4094.

```
• vrrp <1-255> monitor critical-resource <CRM-NAME1> <CRM-NAME2> <CRM-NAME3> <CRM-
NAME4> (action [decrement-priority|increment-priority] {<IF-NAME>|pppoe1|vlan|
wwan1})
```

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
monitor	Enables link monitoring or *Critical Resource Monitoring* (CRM)

critical-resource <CRM-NAME1>	Specifies the name of the critical resource to monitor. VRRP can be configured to monitor maximum of four critical resources. Use the <CRM-NAME2>, <CRM-NAME3>, and <CRM-NAME4> to provide names of the remaining three critical resources. By default VRRP is configured to monitor all critical resources on the device.
action [decrement-priority| increment-priority]	Sets the action on critical resource down event. It is a recursive parameter that sets the action for each of the four critical resources being monitored. • decrement-priority – Decrements the priority of virtual router on critical resource down event • increment-priority – Increments the priority of virtual router on critical resource down event
<IF-NAME>	Optional. Enables interface monitoring • <IF-NAME> – Specify the interface name to monitor
pppoe1	Optional. Enables *Point-to-Point Protocol* (PPP) over Ethernet interface monitoring
vlan <1-4094>	Optional. Enables VLAN (switched virtual interface) interface monitoring • <1-4094> – Specify the VLAN interface ID from 1- 4094.
wwan1	Optional. Enables Wireless WAN interface monitoring

- `vrrp <1-255> timers advertise [<1-255>|centiseconds <25-4095>|msec <250-999>]`

vrrp <1-255>	Configures the virtual router ID from 1- 255. Identifies the virtual router the packet is reporting status for.
timers	Configures the timer that runs every interval
advertise [<1-255>| centiseconds <25-4095>| msec <250-999>]	Configures the VRRP advertisements time interval. This is the interval at which a master sends out advertisements on each of its configured VLANs. • <1-255> – Configures the timer interval from 1- 255 seconds. (applicable for VRRP version 2 only) • centiseconds <25-4095> – Configures the timer interval in centiseconds (1/100th of a second). Specify a value between 25 - 4095 centiseconds (applicable for VRRP version 3 only). • msec <250-999> – Configures the timer interval in milliseconds (1/1000th of a second). Specify a value between 250 - 999 msec (applicable for VRRP version 2 only). Default is 1 second.

- `vrrp version [2|3]`

vrrp version [2|3]	Configures one of the following VRRP versions: • 2 – VRRP version 2 (RFC 3768). This is the default setting. • 3 – VRRP version 3 (RFC 5798 only IPV4) The VRRP version determines the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#vrrp version 3

rfs6000-37FABE(config-profile-default-rfs6000)#vrrp 1 sync-group

rfs6000-37FABE(config-profile-default-rfs6000)#vrrp 1 delta-priority 100

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
 ....................................................
 vrrp 1 timers advertise 1
 vrrp 1 preempt
 vrrp 1 sync-group
 vrrp 1 delta-priority 100
 vrrp version 3
rfs6000-37FABE(config-profile-default-rfs7000)#
```

Related Commands

no	Reverts VRRP settings

7.1.78 vrrp-state-check

Profile Config Commands

Publishes interface via OSPF or BGP based on *Virtual Router Redundancy Protocol* (VRRP) status

VRRP allows automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
vrrp-state-check
```

Parameters

None

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#vrrp-state-check

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
.....................................................................
   no weight
  no timers bgp
  ip default-gateway priority 7500
  bgp-route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 360
 vrrp-state-check
 controller adopted-devices controllers
 alias string $SN B4C7996C8809
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands

no	Disables the publishing of an interface via OSPF/BGP based on VRRP status

7.1.79 virtual-controller

Profile Config Commands

Enables an access point as a *virtual-controller* (VC) or a *dynamic virtual controller* (DVC)

When configured without the 'auto' option, this command manually enables an AP as a VC. The 'auto' option allows dynamic enabling of APs as VCs. When DVC is enabled on an AP's device or profile context, the AP is dynamically enabled as the VC on being elected as the RF-Domain manager.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

NOTE: The DVC feature is supported only on the AP7522, AP7532, AP7562, AP8432, and AP8533 model access points.

Syntax

```
virtual-controller {auto|management-interface}

virtual-controller auto
virtual-controller {management-interface [ip address <IP/M>|vlan <1-4094>]}
```

Parameters

- `virtual-controller auto`

virtual-controller auto	Enables an AP as a virtual-controller • auto – Enables AP as a DVC. When enabled, the AP on being elected as the RF Domain manager takes on the role of the virtual controller. In an RF-Domain, DVC can be enabled on multiple access points. However, only the current RF-Domain manager AP has a running instance of the DVC. This option is applicable only if enabling DVC. **Note:** MLCP discovery does not function on APs enabled as VC or DVCs. Do an explicit "mint link vlan X" on the AP's device/profile context, or "control-vlan X" in the AP's RF-Domain context, to establish MiNT links between the VC and its adopted APs.

- virtual-controller *{management-interface [ip address <IP/M>|vlan <1-4094>]}*

virtual-controller {management-interface [ip address <IP/M>|vlan <1-4094>]}	Enables an AP as a virtual-controller. If enabling DVC, use this option to configure management interface details. • management-interface – Configures the management interface for the DVC. Configuring the management interface ensures failover in case the RF Domain manager is unreachable. • ip address <IP/M> – Specify the management interface IP address. Due to the random nature of DVC, specifying an explicit management interface IP address makes it easier to manage VCs. In case of fail over, this IP address is installed as the secondary IP address on the new VC. • vlan <1-4094> – Optional. Specifies the VLAN from 1 - 4094 on which the management interface IP address is configured. **Note:** For DVC, configuring management-interface ip address is mandatory. However, VLAN configuration is optional. If you configure the *ip address* without specifying the *VLAN*, the system configures the specified ip address as secondary ip on VLAN 1.

Example

```
ap8533-9A1529(config-device-74-67-F7-9A-15-29)#virtual-controller auto

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#virtual-controller management-
interface ip address 110.110.110.120/24

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#virtual-controller management-
interface vlan 100

ap8533-9A1529(config-device-74-67-F7-9A-15-29)#show context | include virtual-
controller
virtual-controller auto
virtual-controller management-interface ip address 110.110.110.120/24
virtual-controller management-interface vlan 100
ap8533-9A1529(config-device-74-67-F7-9A-15-29)#
```

The following example shows the management interface VLAN IP address being configured as the secondary IP address.

```
ap8533-9A1529(config-device-74-67-F7-9A-15-29)#show ip interface brief
-------------------------------------------------------------------------------
INTERFACE          IP-ADDRESS/MASK            TYPE        STATUS   PROTOCOL
-------------------------------------------------------------------------------
vlan1              10.1.1.11/24               primary     UP       up
vlan100            110.110.110.110/24         primary     UP       up
vlan100            110.110.110.120/24         secondary   UP       up
-------------------------------------------------------------------------------
```

7.1.80 wep-shared-key-auth

Profile Config Commands

Enables support for 802.11 WEP shared key authentication

When enabled, devices, using this profile, use a WEP key to access the network. The controller or service platform use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without the recommended adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
wep-shared-key-auth
```

Parameters

None

Example

```
rfs6000-37FABE(config-profile-default-rfs6000)#wep-shared-key-auth

rfs6000-37FABE(config-profile-default-rfs6000)#show context
profile rfs6000 default-rfs6000
 bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
 wep-shared-key-auth
 autoinstall configuration
 autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 interface me1
 interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
 interface ge2
  ip dhcp trust
--More--
rfs6000-37FABE(config-profile-default-rfs6000)#
```

Related Commands

no	Disables support for 802.11 WEP shared key authentication

7.1.81 service

Profile Config Commands

Service commands are used to view and manage configurations. The service commands and their corresponding parameters vary from mode to mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
service [captive-portal-server|cluster|critical-resource|fast-switching|enable|
global-association-list|lldp|memory|meshpoint|pm|power-config|radius|remote-
config|rss-timeout|watchdog|wireless|show]

service captive-portal-server connections-per-ip <3-64>

service cluster master-election immediate

service critical-resource port-mode-source-ip <IP>

service enable [l2tpv3|pppoe|radiusd]

service global-association-list blacklist-interval <1-65535>

service lldp loop-detection

service memory kernel decrease

service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-5>|port-channel
<1-2>|up1]

service pm sys-restart

service power-config [3af-out|force-3at]

service radius dynamic-authorization additional-port <1-65535>

service remote-config apply-delay <0-600>

service rss-timeout <0-86400>

service watchdog

service wireless [anqp-frag-always|anqp-frag-size|ap650|client|cred-cache-sync|
inter-ap-key|noise-immunity|reconfig-on-tx-stall|test|wispe-controller-port]

service wireless anqp-frag-always
service wireless anqp-frag-size <100-1500>
service wireless ap650 legacy-auto-update-image <FILE>
service wireless client tx-deauth on-radar-detect
service wireless cred-cache-sync [full|interval <30-864000>|never|partial]
service wireless test [max-rate|max-retries|min-rate]
service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24,36,48,54,mcs0,
mcs1,.....mcs23]
service wireless inter-ap-key [0 <WORD>|2 <WORD>|<WORD>]
service wireless noise-immunity
service wireless reconfig-on-rx-stall
service wireless test max-retries <0-15>
service wireless wispe-controller-port <1-65535>
```

```
service show cli
```

Parameters

- `service captive-portal-server connections-per-ip <3-64>`

captive-portal-server connections-per-ip <3-64>	Configures the maximum number of simultaneous captive portal connection allowed per IP address • <3-64> – Specify the maximum number of connections per IP address from 3 - 64. The default is 3. **Note:** This command is applicable only to the NX9XXX and NX9600 service platform profiles.

- `service cluster master-election immediate`

cluster master-election immediate	Initiates and completes cluster master election as soon as just one cluster member comes on and is active. This option is disabled by default.

- `service critical-resource port-mode-source-ip <IP>`

critical-resource port-mode-source-ip <IP>	Hard codes a source IP for critical resource management The default is 0.0.0.0 Use this option to define the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. By default, the source address used in ARP packets to detect critical resources is 0.0.0.0. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for port-mode-source-ip monitoring must be different from the IP address configured on the device.

- `service enable [l2tpv3|pppoe|radiusd]`

service enable l2tpv3	Enables L2TPv3 on this profile The L2TPV3 enable/disable option is not supported on AP6522, AP6532, AP6562, AP7161, AP81XX, AP8232, AP8432, AP8533, RFS4000, RFS6000, and NX95XX model devices. It is supported only on AP6521.
service enable pppoe	Enables PPPoE features. When executed on a device, enables PPPoE on the logged device. When executed on a profile, enables PPPoE on all devices using that profile.
service enable radiusd	Enables RADIUSD features. When executed on a device, enables RADIUSD on the logged device. When executed on a profile, enables RADIUSD on all devices using that profile.

- `service global-association-list blacklist-interval <1-65535>`

service global-association-list	Configures global association list related parameters
blacklist-interval <1-65535>	Configures the period for which a client is blacklisted. A client is considered blacklisted after being denied access by the server. • <1-65535> – Specify a value from 1 - 65535 seconds. The default is 60 seconds.

- `service lldp loop-detection`

lldp loop-detection	Enables network loop detection via LLDP. This option is disabled by default.

- `service memory kernel decrease`

service memory kernel decrease	Enables reduction in kernel memory usage. When enabled, firewall flows are reduced by 75% resulting in reduced kernel memory usage. A reboot is required for the option to take effect. This option is disabled by default.

- `service meshpoint loop-prevention-port [<L2-INTERFACE-NAME>|ge <1-4>| port-channel <1-2>]`

meshpoint loop-prevention-port	Limits meshpoint loop prevention to a single port
<L2-INTERFACE-NAME>	Limits meshpoint loop prevention on a specified Ethernet interface • <L2-INTERFACE-NAME> – Specify the layer 2 Ethernet interface name.
ge <1-4>	Limits meshpoint loop prevention on a specified GigabitEthernet interface • ge <1-4> – Specify the GigabitEthernet interface index from 1 - 4.
port-channel <1-2>	Limits meshpoint loop prevention on a specified port-channel interface • port-channel <1-2> – Specify the port-channel interface index from 1 - 2.

- `service pm sys-restart`

pm sys-restart	Enables the *process monitor* (PM) to restart the system when a process fails. This option is enabled by default.

- `service power-config [3af-out|force-3at]`

power-config 3af-out	Enables LLDP power negotiation, but uses 3af power. This option is disabled by default.
power-config force-3at	Disables LLDP negotiation and forces 802.3at power configuration. This option is disabled by default.

- `service radius dynamic-authorization additional-port <1-65535>`

radius dynamic-authorization additional-port <1-65535>	Configures an additional UDP port used by the device to listen for dynamic authorization messages • <1-65535> – Specify a value from 1 - 65535. The default is 3799. The Cisco *Identity Services Engine* (ISE) server uses port 1700.

- `service remote-config apply-delay <0-600>`

remote-config apply-delay <0-600>	Delays configuration of a remote device (after it becomes active) by the specified time period • <0-600> – Specify a value from 0 - 600 seconds. The default is 0 seconds.

- `service rss-timeout <0-86400>`

rss-timeout <0-86400>	Configures the duration, in seconds, for which an adopted access point will continue to provide wireless functions even after loosing controller adoption. • <0-86400> – Specify a value from 0 - 86400 seconds. The default is 300 seconds.

- `service watchdog`

watchdog	Enables the watchdog. This feature is enabled by default. Enabling the watchdog option implements heartbeat messages to ensure other associated devices are up and running and capable of effectively inter-operating with the controller.

- `service wireless anqp-frag-always`

wireless anqp-frag-always	Enables fragmentation of all ANQP packets. This option is disabled by default.

- `service wireless anqp-frag-size <100-1500>`

wireless anqp-frag-size <100-1500>	Configures the ANQP packet fragment size • <100-1500> – Specify a value from 100 - 1500. The default is 1200.

- `service wireless client tx-deauth on-radar-detection`

wireless client	Configures wireless client and stations related settings
tx-deauth on-radar-detection	Enables access points to transmit deauth to clients when changing channels on radar detection. This option is enabled by default.

- `service wireless cred-cache-sync [full|interval <30-864000>|never|partial]`

wireless cred-cache-sync	Configures the credential cache's synchronization parameters. The parameters are: full, interval, never, and partial.
full	Enables synchronization of all credential cache entries
interval <30-864000>	Sets the interval, in seconds, at which the credential cache is synchronized • <30-864000> – Specify a value from 30 - 864000 seconds. The default is 1200 seconds.
never	Disables credential cache entry synchronization for all associated clients other than roaming clients. This is the default setting.
partial	Enables partial synchronization of parameters for associated clients, with credential cache close to aging out

- `service wireless inter-ap-key [0 <WORD>|2 <WORD>|<WORD>]`

wireless inter-ap-key	Configure encryption key used for securing inter-ap messages. This option is disabled by default.
[0<WORD>| 2<WORD>|<WORD>]	Specify a clear text or encrypted key.

- `service wireless noise-immunity`

wireless noise-immunity	Polls for status and reconfigures radio in case of receive stall. This option is enabled by default.

- `service wireless reconfig-on-rx-stall`

wireless reconfig-on-rx-stall	Enables noise immunity on the radio

- `service wireless test [max-rate|min-rate] [1,2,5.5,6,11,12,18,24,36,48, 54,mcs0,mcs1,.....mcs23]`

wireless test	Configures the serviceability parameters used for testing
[max-rate|min-rate]	Configures the maximum and minimum data rates for clients using rate-scaling. The 'max-rate' and min-rate' options are disabled by default.
[1,2,5.5,....mcs23]	Select the maximum and minimum data rates applicable.

- `service wireless test max-retries <0-15>`

wireless test	Configures the serviceability parameters used for testing
max-retries <0-15>	Configures the maximum number of retries per packet from 0 - 15. The default is 0.

- `service wireless wispe-controller-port <1-65535>`

wispe-controller-port <1-65535>	Resets the *WIreless Switch Protocol Enhanced* (WISPe) controller port. This is the UDP port used to listen for WISPe. • <1-65535> – Specify a value from 1 - 65535. The default is 24756.

- `service show cli`

show cli	Displays running system configuration details • cli – Displays the CLI tree of the current mode

Example

```
rfs6000-37FABE(config-profile-testrfs6000)#service radius dynamic-authorization
additional-port 1700

rfs6000-37FABE(config-profile-testrfs6000)#show context
profile rfs6000 testrfs6000
 service radius dynamic-authorization additional-port 1700
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
--More--
rfs6000-37FABE(config-profile-testrfs6000)#
```

Related Commands

no	Removes or resets service command parameters

7.1.82 zone

Profile Config Commands

Configures the zone for devices using this profile. The zone can also be configured on the device's self context.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
zone <NAME>
```

Parameters

- `zone <NAME>`

zone <NAME>	Configures the device's zone/area • <NAME> – Specify the zone/areaname.

Example

```
nx9500-6C8809(config-profile-testNX9000)#szone Ecospace

nx9500-6C8809(config-profile-testNX9000)#show context include-factory | include
zone
 zone Ecospace
nx9500-6C8809(config-profile-testNX9000)#
```

Related Commands

no	Removes the zone configured on this profile or device

7.2 Device Config Commands

PROFILES

Use the (config) instance to configure device specific parameters

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#<DEVICE-TYPE> <MAC>
<DEVICE>(config-device-<MAC>)#?
Device Mode commands:
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  adoption                                 Adoption configuration
  adoption-mode                            Configure the adoption mode for the
                                           access-points in this RF-Domain
  adoption-site                            Set system's adoption site
  alias                                    Alias
  application-policy                       Application Policy configuration
  area                                     Set name of area where the system
                                           is located?
  arp                                      Address Resolution Protocol (ARP)
  auto-learn                               Auto learning
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bridge                                   Ethernet bridge
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  channel-list                             Configure channel list to be
                                           advertised to wireless clients
  cluster                                  Cluster configuration
  configuration-persistence                Enable persistence of configuration
                                           across reloads (startup config
                                           file)
  contact                                  Configure the contact
  controller                               WLAN controller configuration
  country-code                             Configure the country of operation
  critical-resource                        Critical Resource
  crypto                                   Encryption related commands
  database                                 Database command
  device-upgrade                           Device firmware upgrade
  device-onboard                           Device-onboarding configuration
  dot1x                                    802.1X
  dpi                                      Enable Deep-Packet-Inspection
                                           (Application Assurance)
  dscp-mapping                             Configure IP DSCP to 802.1p
                                           priority mapping for untagged
  eguest-server                            Enable EGuest Server functionality
                                           frames
  email-notification                       Email notification configuration
  enforce-version                          Check the firmware versions of
                                           devices before interoperating
  environmental-sensor                     Environmental Sensors Configuration
  events                                   System event messages
  export                                   Export a file
  file-sync                                File sync between controller and
                                           adoptees
  floor                                    Set the floor within a area where
                                           the system is located
  geo-coordinates                          Configure geo coordinates for this
                                           device
  gre                                      GRE protocol
  hostname                                 Set system's network name
  http-analyze                             Specify HTTP-Analysis configuration
  interface                                Select an interface to configure
```

```
ip                                  Internet Protocol (IP)
ipv6                                Internet Protocol version 6 (IPv6)
l2tpv3                              L2tpv3 protocol
l3e-lite-table                      L3e lite Table
lacp                                LACP commands
layout-coordinates                  Configure layout coordinates for
                                    this device
led                                 Turn LEDs on/off on the device
led-timeout                         Configure the time for the led to
                                    turn off after the last radio state
                                    change
legacy-auto-downgrade               Enable device firmware to auto
                                    downgrade when other legacy devices
                                    are detected
legacy-auto-update                  Auto upgrade of legacy devices
license                             License management command
lldp                                Link Layer Discovery Protocol
load-balancing                      Configure load balancing parameter
location                            Configure the location
logging                             Modify message logging facilities
mac-address-table                   MAC Address Table
mac-auth                            802.1X
mac-name                            Configure MAC address to name
                                    mappingss
management-server                   Configure management server address
memory-profile                      Memory profile to be used on the
                                    device
meshpoint-device                    Configure meshpoint device
                                    parameters
meshpoint-monitor-interval          Configure meshpoint monitoring
                                    interval
min-misconfiguration-recovery-time  Check controller connectivity after
                                    configuration is received
mint                                MiNT protocol
mirror                              Mirroring
misconfiguration-recovery-time      Check controller connectivity after
                                    configuration is received
mpact-server                        MPACT server configuration
neighbor-inactivity-timeout         Configure neighbor inactivity
                                    timeout
neighbor-info-interval              Configure neighbor information
                                    exchange interval
no                                  Negate a command or set its
                                    defaults
noc                                 Configure the noc related setting
nsight                              NSight
nsight-sensor                       Enable sensor for Nsight
ntp                                 Ntp server A.B.C.D
offline-duration                    Set duration for which a device
                                    remains unadopted before it
                                    generates offline event
otls                                Omnitrail Location Server
override-wlan                       Configure RF Domain level overrides
                                    for wlan
power-config                        Configure power mode
preferred-controller-group          Controller group this system will
                                    prefer for adoption
preferred-tunnel-controller         Tunnel Controller Name this system
                                    will prefer for tunneling extended
                                    vlan traffic
radius                              Configure device-level radius
                                    authentication parameters
raid                                RAID
remove-override                     Remove configuration item override
                                    from the device (so profile value
                                    takes effect)
rf-domain-manager                   RF Domain Manager
router                              Dynamic routing
```

```
rsa-key                                  Assign a RSA key to a service
sensor-server                            AirDefense sensor server
                                         configuration
slot                                     PCI expansion Slot
spanning-tree                            Spanning tree
timezone                                 Configure the timezone
traffic-class-mapping                    Configure IPv6 traffic class to
                                         802.1p priority mapping for
                                         untagged frames
traffic-shape                            Traffic shaping
trustpoint                               Assign a trustpoint to a service
tunnel-controller                        Tunnel Controller group this
                                         controller belongs to
use                                      Set setting to use
vrrp                                     VRRP configuration
vrrp-state-check                         Publish interface via OSPF/BGP only
                                         if the interface VRRP state is not
                                         BACKUP
wep-shared-key-auth                      Enable support for 802.11 WEP
                                         shared key authentication
zone                                     Configure Zone name

clrscr                                   Clears the display screen
commit                                   Commit all changes made in this
                                         session
do                                       Run commands from Exec mode
end                                      End current mode and change to EXEC
                                         mode
exit                                     End current mode and down to
                                         previous mode
help                                     Description of the interactive help
                                         system
revert                                   Revert changes
service                                  Service Commands
show                                     Show running system information
write                                    Write running configuration to
                                         memory or terminal

<DEVICE>(config-device-<MAC>)#
```

The following table summarizes device configuration mode commands:

Command	Description	Reference
adopter-auto-provisioning-policy-lookup	Enables the use of a centralized auto provisioning policy on this device	*page 7-11*
adoption	Configures a minimum and maximum delay time in the initiation of the device adoption process	*page 7-13*
adoption-site	Sets the device's adoption site name	*page 7-464*
alias	Configures network, VLAN, and service aliases on a device	*page 7-15*
application-policy	Associates a RADIUS server provided application policy with this device. When associated, the application policy allows wireless clients (MUs) to always find the RADIUS-supplied application policy in the dataplane.	*page 7-22*
area	Sets the name of area where the system is deployed	*page 7-465*
arp	Configures ARP parameters	*page 7-25*

Command	Description	Reference
auto-learn	Enables controllers or service platforms to maintain a local configuration record of devices requesting adoption and provisioning. The command also enables learning of a device's host name via DHCP options.	*page 7-27*
autogen-uniqueid	When executed in the device configuration mode, this command generates a unique ID for the logged device	*page 7-28*
autoinstall	Autoinstalls firmware image and configuration setup parameters	*page 7-30*
bridge	Configures Ethernet Bridging parameters	*page 7-31*
captive-portal	Configures captive portal advanced Web page upload on this profile	*page 7-62*
cdp	Operates CDP on the device	*page 7-63*
channel-list	Configures channel list advertised to wireless clients	*page 7-466*
cluster	Sets cluster configuration	*page 7-64*
configuration-persistence	Enables configuration persistence across reloads	*page 7-67*
contact	Sets contact information	*page 7-467*
controller	Configures a WLAN's wireless controller or service platform	*page 7-68*
country-code	Configures wireless controller or service platform's country code	*page 7-468*
critical-resource	Monitors user configured IP addresses and logs their status	*page 7-72*
crypto	Configures data encryption protocols and settings	*page 7-80*
database	Backs up captive-portal and/or NSight database to a specified location and file and configures a low-disk-space threshold value	*page 7-143*
device-upgrade	Configures device firmware upgrade settings on this device	*page 7-145*
diag	Enables looped packet logging	*page 7-147*
dot1x	Configures 802.1x standard authentication controls	*page 7-148*
dpi	Enables *Deep Packet Inspection* (DPI) on this device	*page 7-150*
dscp-mapping	Configures IP *Differentiated Services Code Point* (DSCP) to 802.1p priority mapping for untagged frames	*page 7-153*
eguest-server (VX9000 only)	Enables the EGuest daemon when executed without the 'host' option	*page 7-154*
eguest-server (NOC Only)	Points to the EGuest server, when executed along with the 'host' option	*page 7-155*
email-notification	Configures e-mail notification settings	*page 7-156*
enforce-version	Checks the device firmware version before attempting connection	*page 7-158*
environmental-sensor	Configures the environmental sensor device settings. If the device is an environmental sensor, use this command to configure its settings.	*page 7-159*
events	Enables system event message generation and forwarding	*page 7-161*
export	Enables export of startup.log file after every boot	*page 7-162*
file-sync	Configures parameters enabling syncing of trustpoint/wireless-bridge certificate between the staging-controller and its adopted access points	*page 7-163*
floor	Sets the floor name where the system is located	*page 7-164*

Command	Description	Reference
geo-coordinates	Configures the geographic coordinates for this device	*page 7-470*
gre	Enables GRE tunneling on this device	*page 7-166*
hostname	Sets a system's network name	*page 7-471*
http-analyze	Enables HTTP analysis on this device	*page 7-177*
interface	Selects an interface to configure	*page 7-180*
ip	Configures IPv4 components	*page 7-348*
ipv6	Configures IPv6 components	*page 7-358*
l2tpv3	Defines the *Layer 2 Tunnel Protocol* (L2TP) protocol for tunneling Layer 2 payloads using *Virtual Private Networks* (VPNs)	*page 7-362*
l3e-lite-table	Configures L3e Lite Table with this profile	*page 7-364*
lacp	Configures an LACP-enabled peer's system-priority value. LACP uses this system-priority value along with the peer's MAC address to form the peer's system ID.	*page 7-472*
layout-coordinates	Configures layout coordinates	*page 7-473*
led	Turns LEDs on or off	*page 7-365*
led-timeout	Configures the LED-timeout timer in the device or profile configuration mode	*page 7-366*
legacy-auto-downgrade	Enables legacy device firmware to auto downgrade	*page 7-368*
legacy-auto-update	Auto updates AP7161 legacy device firmware	*page 7-369*
license	Adds device feature licenses	*page 7-474*
lldp	Configures *Link Layer Discovery Protocol* (LLDP) settings for this device	*page 7-370*
load-balancing	Configures load balancing parameters.	*page 7-372*
location	Configures the system's location (place of deployment)	*page 7-477*
logging	Enables message logging	*page 7-377*
mac-address-table	Configures the MAC address table	*page 7-379*
mac-auth	Enables 802.1x authentication of hosts on this device	*page 7-381*
mac-name	Configures MAC address to device name mappings	*page 7-478*
management-server	Configures a management server with this profile	*page 7-384*
memory-profile	Configures memory profile used on the device	*page 7-385*
meshpoint-device	Configures meshpoint device parameters	*page 7-386*
meshpoint-monitor-interval	Configures meshpoint monitoring interval	*page 7-388*
min-misconfiguration-recovery-time	Configures the minimum device connectivity verification time	*page 7-389*
mint	Configures MiNT protocol settings	*page 7-390*

Command	Description	Reference
misconfiguration-recovery-time	Verifies device connectivity after a configuration is received	page 7-397
neighbor-inactivity-timeout	Configures neighbor inactivity timeout value	page 7-398
neighbor-info-interval	Configures the neighbor information exchange interval	page 7-399
no	Negates a command or resets values to their default settings	page 7-479
noc	Configures NOC settings	page 7-402
nsight	Configures NSight database statistics related parameters. Use this command to set the interval at which data is updated by the RF Domain managers to the NSight server. This command is applicable only on the NX95XX series and NX9600 service platforms and is configured on the NSight server.	page 7-480
ntp	Configures NTP server settings	page 7-408
offline-duration	Sets the duration, in minutes, for which a device remains unadopted before it generates offline event	page 7-414
override-wlan	Configures WLAN RF Domain level overrides on the logged device	page 7-484
power-config	Configures power mode features	page 7-415
preferred-controller-group	Specifies the wireless controller or service platform group the system prefers for adoption	page 7-417
preferred-tunnel-controller	Configures the tunnel wireless controller or service platform preferred by the system for tunneling extended VLAN traffic	page 7-418
radius	Configures device-level RADIUS authentication parameters	page 7-419
remove-override	Removes device overrides	page 7-486
rf-domain-manager	Enables the RF Domain manager	page 7-420
router	Configures dynamic router protocol settings.	page 7-421
rsa-key	Assigns a RSA key to SSH	page 7-488
sensor-server	Configures an AirDefense sensor server	page 7-489
spanning-tree	Enables spanning tree commands on the logged device	page 7-423
traffic-class-mapping	Maps the IPv6 traffic class value of incoming IPv6 untagged packets to 802.1p priority	page 7-426
traffic-shape	Enables traffic shaping and configures traffic shaping parameters on this device	page 7-428
trustpoint (device-config-mode)	Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server, etc.	page 7-491
timezone	Configures wireless controller or service platform's time zone settings	page 7-490
tunnel-controller	Configures the tunneled WLAN (extended VLAN) wireless controller or service platform's name	page 7-436
use	Associates different policies and settings with this device	page 7-437
vrrp	Configures VRRP group settings	page 7-443

Command	Description	Reference
vrrp-state-check	Publishes interface via OSPF or BGP based on *Virtual Router Redundancy Protocol* (VRRP) status	*page 7-447*
wep-shared-key-auth	Enables support for 802.11 WEP shared key authentication	*page 7-450*
raid	Enables alarm on the array. This command is supported only on the NX9500 series service platform.	*page 7-493*

7.2.1 adoption-site

Device Config Commands

Sets the device's adoption site name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
adoption-site <SITE-NAME>
```

Parameters

- `adoption-site <SITE-NAME>`

adoption-site <SITE-NAME>	Sets the device's adoption site name

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#adoption-site SanJoseMainOffice
```

Related Commands

no	Disables or reverts settings to their default

7.2.2 area

Device Config Commands

Sets the physical area where the device (controller, service platform, or access point) is deployed. This can be a building, region, campus or other area that describes the deployment location of the device. Assigning an area name is helpful when grouping devices in RF Domains and profiles, as devices in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
area <AREA-NAME>
```

Parameters

- `area <AREA-NAME>`

area <AREA-NAME>	Sets the physical area where the device is deployed <AREA-NAME> – Specify the area name (should not 64 characters in length).

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#area RMZEcoSpace

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7131-4AA708
 area RMZEcospace
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Disables or reverts settings to their default

7.2.3 channel-list

Device Config Commands

Configures the channel list advertised to wireless clients

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
channel-list [2.4GHz|5GHz|dynamic]
channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]
```

Parameters

- `channel-list [2.4GHz <CHANNEL-LIST>|5GHz <CHANNEL-LIST>|dynamic]`

channel-list	Configures the channel list advertised to wireless clients
2.4GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in 2.4 GHz • <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens.
5GHz <CHANNEL-LIST>	Configures the channel list advertised by radios operating in 5.0 GHz • <CHANNEL-LIST> – Specify a list of channels separated by commas or hyphens.
dynamic	Enables dynamic (neighboring access point based) update of configured channel list

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#channel-list 2.4GHz 1,2

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7131-4AA708
 area RMZEcospace
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Resets the channel list configuration

7.2.4 contact

Device Config Commands

Defines an administrative contact for a deployed device (controller, service platform, or access point)

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
contact <WORD>
```

Parameters

- `contact <WORD>`

contact <WORD>	Specify the administrative contact name (should not exceed 64 characters in length)

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#contact Bob+1-631-738-5200

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7131-4AA708
 area RMZEcospace
 contact Bob+1-631-738-5200
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Resets the administrative contact name

7.2.5 country-code

Device Config Commands

Defines the two digit country code for legal device deployment

Configuring the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
country-code <WORD>
```

Parameters

- `country-code <COUNTRY-CODE>`

country-code <COUNTRY-CODE>	Defines the two digit country code for legal device deployment • <COUNTRY-CODE> – Specify the two letter ISO-3166 country code.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#country-code us

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7131-4AA708
 area RMZEcospace
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes the configured country code

7.2.6 floor

Device Config Commands

Sets the building floor name representative of the location within the area or building the device (controller, service platform, or access point) is physically deployed. Assigning a building floor name is helpful when grouping devices in RF Domains and profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
floor <FLOOR-NAME> <1-4094>
```

Parameters

- `floor <FLOOR-NAME> <1-4094>`

floor <FLOOR-NAME> <1-4094>	Sets the building floor name where the device is deployed • <1-4094> – Sets a numerical floor designation in respect to the floor's actual location within a building. Specify a value from 1 - 4094. The default setting is the 1st floor.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#floor 5thfloor

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname ap7131-4AA708
 area RMZEcospace
 floor 5thfloor
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes device's location floor name

7.2.7 geo-coordinates

Device Config Commands

Configures the geographic coordinates for this device. Specifies the exact location of this device in terms of latitude and longitude coordinates.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>
```

Parameters

- `geographic coordinates <-90.0000-90.0000> <-180.0000-180.0000>`

geographic coordinates	Configures the geographic coordinates for this device • <-90.0000-90.0000> – Specify the device's latitude coordinate from -90.0000 to 90.0000. When looking at a floor map, latitude lines specify the *east-west* position of a point on the Earth's surface. • <-180.0000-180.0000> – Specify the device's longitude coordinate from -180.0000 to 180.0000. When looking at a floor map, longitude lines specify the *north-south* position of a point on the Earth's surface.

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#geo-coordinates -90.0000 166.0000

rfs4000-229D58(config-device-00-23-68-22-9D-58)#show context
rfs4000 00-23-68-22-9D-58
 use profile default-rfs4000
 use rf-domain default
 hostname rfs4000-229D58
 geo-coordinates -90.0000 166.0000
 license AP DEFAULT-6AP-LICENSE
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 ip default-gateway 192.168.13.2
 ip default-gateway priority static-route 20
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 192.168.13.9/24
  ip address 192.168.0.1/24 secondary
  ip dhcp client request options all
 use client-identity-group ClientIdentityGroup
 logging on
 logging console warnings
 logging buffered warnings
rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

Related Commands

no	Removes device's geographic coordinates

7.2.8 hostname

Device Config Commands

Sets the system's network name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
hostname <WORD>
```

Parameters

- `hostname <WORD>`

hostname <WORD>	Sets the name of the managing wireless controller, service platform, or access point. This name is displayed when accessed from any network.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#hostname TechPubAP7131

The hostname has changed from 'ap7131-4AA708' to 'TechPubAP7131'

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes device's hostname

7.2.9 lacp

Device Config Commands

Configures an LACP-enabled peer's system priority value. LACP uses this system priority value along with the peer's MAC address to form the system ID. In a LAG, the peer with the lower system ID initiates LACP negotiations with another peer. In scenarios, where both peers have the same system-priority value assigned, the peer with the lower MAC gets precedence.

NOTE: For more information on enabling link aggregation, see *lacp* and *lacp-channel-group*.

Supported in the following platforms:

- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
lacp system-priority <1-65535>
```

Parameters

- `lacp system-priority <1-65535>`

lacp system-priority <1-65535>	Configures the LACP system priority value • <1-65535> – Specify a value from 1 - 65535. Lower the value, higher is the priority. Therefore, '1' and '65535' indicate highest and lowest system-priority values respectively. The default value is 32768.

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#lacp system-priority 1

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory |
include lacp
 lacp system-priority 1
  lacp-channel-group 1 mode active
  lacp port-priority 2
  lacp-channel-group 1 mode active
  lacp port-priority 2
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands

no	Removes this device's configured system-priority value

7.2.10 layout-coordinates

Device Config Commands

Configures X and Y layout coordinates for the device

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>
```

Parameters

- `layout-coordinates <-4096.0-4096.0> <-4096.0-4096.0>`

layout-coordinates	Configures X and Y layout coordinates for the device
<-4096.0-4096.0>	Specify the X coordinate from -4096 - 4096.0
<-4096.0-4096.0>	Specify the Y coordinate from -4096 - 4096.0

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#layout-coordinates 1.0 2.0

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes device's layout co-ordinates

7.2.11 license

Device Config Commands

Adds a license pack on the device for the specified feature (AP/AAP/ADSEC/HTANLT/WEBF/NSIGHT/NSIGHT-PER/EGUEST-DEV)

The WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers may or may not be grouped to form clusters. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

The NOC controllers and/or site controllers can both have license packs installed. Adoption of APs by the NOC and site controllers depends on the number of licenses available on each of these controllers.

The NOC controllers and/or site controllers can both have license packs installed. When a AP is adopted by a site controller, the site controller pushes a license on to the AP. The various possible scenarios are:

- AP licenses installed only on NOC controller:

  The NOC controller provides the site controllers with AP licenses, ensuring that per platform limits are not exceeded.

- AP licenses installed on site controller:

  The site controller uses its installed licenses, and then asks the NOC controller for additional licenses in case of a shortage.

  In a hierarchical and centrally managed network, the NOC controller can pull unused AP licenses from site controllers and relocate to other site controllers when required.

- AP licenses installed on any member of a site cluster:

  The site controller shares installed and borrowed (from the NOC) licenses with other controllers within a site cluster.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
license <WORD> <LICENSE-KEY>
```

Parameters

- `license <WORD> <LICENSE-KEY>`

<WORD>	Specify the feature name (AP/AAP/ADSEC/HTANLT/WEBF/NSIGHT/NSIGHT-PER/ EGUEST-DEV) for which license is added AP License: This is the license key required for AP adoptions. The number of APs that can be adopted depends on the installed license count. If the installed license count is 10 APs and the number of AP adoptions is 5, 5 additional APs can still be adopted under the terms of the license. AAP License: This is the license key required for AAP adoptions. The number of AAPs that can be adopted depends on the installed license count. If the installed license count is 10 APs and the number of AAP adoptions is 5, 5 additional AAPs can still be adopted under the terms of the license. ADSEC License: This is the license key required to install the Role Based Firewall feature and increase the number of IPSec VPN tunnels. The number of IPSec tunnels varies by platform. HTANLT: This is the license key required to install Analytics (an enhanced statistical management tool) for NX95XX series service platforms. WEBF License: This is the license key required to install the Web filtering feature. Web filtering is used to restrict access to specific resources on the Internet. NSIGHT/NSIGHT-PER Licenses: This is the license key required to install NSight on a supported service platform. The NSight UI displays a comprehensive, day-to-day overview of the network in a graphical, visually interactive, and easy-to-use format. However, NSight being a licensed service, on expiration of the first 120 days grace period, the NSight server's NSight UI can be launched *only on the application* of the *NSight* or *NSight-Per* (NSight Perpetual) license. The difference between the *NSight* and *NSight-Per* licenses is that the first one has an expiration date, whereas the latter doesn't have an expiration date. Once purchased and applied, the NSight-Per license is active forever, and is therefore ideally suited for a Replica-set, NSight deployment, where it is essential that the license is perpetually active and synched across the NSight servers and their primary and secondary databases. **Note:** NSight is supported only on NX9500, NX9510, NX9600 model service platforms, and the VX9000 virtual controller. EGUEST-DEV License - This is the per-device license key installed on the EGuest server. Once installed the EGuest feature is activated. The EGuest-DEV license defines the number of APs supported by each EGuest server. The maximum limit for per-device license is 100,000. The EGuest server is supported only on the VX9000 platform.
<LICENSE-KEY>	Specify the license key.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#license ap aplicensekey@1234
aplicensekey@123

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicensekey@1234 aplicensekey@123
 location SanJose
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#license NSIGHT 62e512ae6cb74689df
253a03efe493f375597b67c70ee0b7c30655256b1322d064ca8dfaecedc450

VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#license EGUEST-DEV
5f06f09e8209cba1fc7db70681fe78ba2707bbcd6ca2e8f8a31fe5b7e2e778c8b0d0ee3994f800ad
VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#commit write


VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#show context include-factory |
include license
 license EGUEST-DEV
5f06f09e8209cba1fc7db70681fe78ba2707bbcd6ca2e8f8a31fe5b7e2e778c8b0d0ee3994f800ad
VX-EGuest-DB(config-device-14-A0-19-06-AB-10)#
```

7.2.12 location

Device Config Commands

Sets the location where a managed device (controller, service platform, or access point) is deployed. This is the location of the device with respect to the RF Domain it belongs.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
location <WORD>
```

Parameters

- `location <WORD>`

<WORD>	Specify the managed device's location as part of its RF Domain configuration

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#location SanJose

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location SanJose
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes a managed device's location

7.2.13 mac-name

Device Config Commands

Configures a client name to MAC address mapping. Use this command to assign a user-friendly name to the device (controller, service platform, or access point) and map it to the device's MAC address.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mac-name <MAC> <NAME>
```

Parameters

- `mac-name <MAC> <NAME>`

mac-name <MAC> <NAME>	Maps a user-friendly name to the device's MAC address • <MAC> – Specify the device's MAC address. • <NAME> – Specify the 'friendly' name used for the specified MAC address. This is the name used in events and statistics logs.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#mac-name 00-04-96-4A-A7-08
5.8TestAP

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 area RMZEcospace
 floor 5thfloor
 layout-coordinates 1.0 2.0
 location SanJose
 contact Bob+1-631-738-5200
 country-code us
 channel-list 2.4GHz 1,2
 mac-name 00-04-96-4A-A7-08 5.8TestAP
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes the device's friendly name to MAC address mapping

7.2.14 no

Device Config Commands

Negates a command or resets values to their default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [adopter-auto-provisioning-policy-lookup|adoption-site|alias|application-
policy|area|arp|auto-learn-staging-config|autoinstall|bridge|captive-portal|
cdp|channel-list|cluster|configuration-persistence|contact|controller|
country-code|critical-resource|crypto|database-backup|device-upgrade|dot1x|
dpi|dscp-mapping|email-notification|environmental-sensor|events|export|
file-sync|floor|geo-coordinates|gre|hostname|http-analyze|interface|ip|ipv6|
l2tpv3|l3-lite-table|lacp|layout-coordinates|led|led-timeout|
legacy-auto-downgrade|legacy-auto-update|license|lldp|load-balancing|location|
logging|mac-address-table|mac-auth|mac-name|management-server|memory-profile|
meshpoint-device|meshpoint-monitor-interval|min-misconfiguration-recovery-time|
mint|mirror|misconfiguration-recovery-time|mpact-server|noc|nsight||ntp|
offline-duration|override-wlan|power-config|preferred-controller-group|
preferred-tunnel-controller|radius|raid|rf-domain-manager|router|rsa-key|
sensor-server|slot|spanning-tree|timezone|traffic-class-mapping|traffic-shape|
trustpoint|tunnel-controller|use|vrrp|vrrp-state-check|wep-shared-key-auth|
service]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or resets the logged device's settings based on the parameters passed

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no area

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#no contact
```

7.2.15 nsight

Device Config Commands

Configures NSight database related parameters. Use this command to configure the data-update periodicity, number of applications posted to the NSight server for a wireless client, and the duration for which data is stored in the NSight database's buckets. These parameters impact the amount of data stored in the NSight DB and interval at which data is aggregated and expired within the NSight DB. For more information on data aggregation and expiration, see *(Data Aggregation and Expiration)*.

Configure these parameters in the NSight server's device configuration mode.

Supported in the following platforms:

- Service Platforms — NX9500, NX9510, NX9600, VX9000

Syntax

```
nsight database [statistics|summary]

nsight database statistics [avc-update-interval|max-apps-per-client|update-interval|wireless-clients-update-interval]

nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-interval] [120|30|300|60|600]

nsight database statistics max-apps-per-client <1-1000>

nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>
```

Parameters

```
• nsight database statistics [avc-update-interval|update-interval|wireless-clients-update-interval] [120|30|300|60|600]
```

nsight database statistics	Configures NSight database statistics related parameters
avc-update-interval	Configures the interval, in seconds, at which *Application Visibility and Control* (AVC) statistics is updated to the NSight database. This interval represents the rate at which AVC-related data is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see *(Data Aggregation and Expiration)*. When configured, RF Domain managers posting AVC-related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the *avc-update-interval* configured here.
update-interval	Configures the interval, in seconds, at which data is updated to the NSIght server. This interval represents the rate at which data (excluding AVC and wireless-clients related statistics) is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see *(Data Aggregation and Expiration)*. When configured, RF Domain managers posting data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the *update-interval* configured here. **Note:** Use the '*avc-update-interval*' and '*wireless-clients-update-interval*' keywords to configure update interval for *AVC-related* and *wireless-clients* related information respectively.

wireless-clients-update-interval	Configures the interval, in seconds, at which wireless-client statistics is updated to the NSIght server. This interval represents the rate at which wireless-clients related statistics is inserted in the NSight database's first bucket. This first bucket data is referred to as the RAW records. A bucket is a database collection that holds statistical data on a per RF Domain basis. For more information, see *(Data Aggregation and Expiration)*. When configured, RF Domain managers posting wireless-client related data to the NSight server receive a reply from the NSight server intimating the next update time. The NSight server calculates the 'next update time' based on the *wireless-clients-update-interval* configured here.
[120|30|300|60|600]	The following keywords are common to all of the above parameters: • 120 – Sets the data-update periodicity as 120 seconds (2 minutes) • 30 – Sets the data-update periodicity as 30 seconds • 300 – Sets the data-update periodicity as 300 seconds (5 minutes). This is the default setting for the *'avc-update-interval'* and '*wireless-clients-update-interval*' parameters. • 60 – Sets the data-update periodicity as 60 seconds (1 minute). This is the default setting for the '*update-interval*' parameter. • 600 – Sets the data-update periodicity as 600 seconds (10 minutes)

- `nsight database statistics max-apps-per-client <1-1000>`

nsight database statistics	Configures NSight database statistics related parameters
max-apps-per-client	Configures the maximum number of applications per wireless-client to be posted to the NSight server within the configured data-update interval. This information is included in the AVC statistics posted by RF Domain managers to the NSIght server.
<1-1000>	Specify the number of applications posted from 1 - 1000. The default is 10 applications per wireless client.

- `nsight database summary duration <1-24> <1-168> <1-2160> <24-26280>`

nsight database summary	Configures the NSight database's per-bucket data storage duration
duration <1-24> <1-168> <1-2160> <24-26280>	Configures the duration for which data is stored on a per-bucket basis • <1-24> – Specify the *bucket 1* duration from 1 - 24 hours (i.e. 1 hour to 1 day). The default is 8 hours. • <1-168> – Specify the *bucket 2* duration from 1 - 168 hours (i.e. 1 hour to 7 days). The default is 24 hours. • <1-2160> – Specify the *bucket 3* duration from 1 - 2160 hours (i.e. 1 hour to 90 days). The default is 7 days (168 hours). • <24-26280> – Specify the *bucket 4* duration from 24 - 26280 hours (i.e. 1 day to 3 years). The default is 365 days (1 year). **Note:** A bucket is a database collection that holds statistical data for each RF Domain within the network. (Note, only those RF Domain's that are using an NSight policy with the NSight server host configured will post data to the NSight server. For more information, see *use* in the RF Domain configuration mode.) NSight database has four (4) buckets. The data from each bucket is aggregated and pushed to the next bucket once the data storage duration, specified for the bucket, has exceeded. For more information on data aggregation, see *(Data Aggregation and Expiration)*.

Usage Guidelines (Data Aggregation and Expiration)

Data Aggregation:

The NSight functionality, a data analytics tool, analyzes data that is generated periodically by the nodes within the managed wireless LAN. For large WLAN networks, generating significantly large amount of data, storing data forever is neither feasible nor beneficial. Therefore, older statistics are summarized into aggregated (averaged) records. All records, for a fixed time period in past, are summarized into one record by taking an average of them. Although this causes a loss in the data's granularity, average numbers for any given time period is still available.

Statistical data periodically posted by RF Domain managers to the NSight server are stored in buckets (database collections) within the NSight database. There are four buckets in total. These are:

- First bucket (termed as the RAW bucket) - B1
- Second bucket - B2
- Third bucket - B3
- Fourth bucket - B4

On completion of the data storage duration, records from a bucket are aggregated (at a fixed rate) and inserted into the next bucket. The rate at which records are aggregated into the next bucket becomes the next bucket's granularity. For example, the B1 records (that have exceeded the data storage duration configured for B1) are aggregated (at the rate specified) and inserted into B2. Similarly, data from B2 are aggregated into B3, and from B3 to B4. The fixed rate of aggregation (or granularity) AND default storage duration for each bucket is as follows:

- B1: storage duration 8 hours
- B2: granularity 10 minutes / storage duration 24 hours
- B3: granularity 1 hour / storage duration 7 days
- B4: granularity 1 day / storage duration 1 year

Let us consider (with default update-interval settings) the growth of any one of the statistical buckets.

- Since B1's default data storage duration is 8 hours, B1 will hold a maximum of 960 records per RF Domain after 8 hours (updated at the rate of 30 seconds).
- Since B2's granularity is 10 minutes, every 10 minutes 20 records from the B1 will be aggregated into a single record and inserted into B2.
- Since B2's default storage duration is 24 hours, it will contain a maximum of 144 records per RF Domain after 24 hours.
- Since B3's granularity is 1 hour, every hour 6 records from B2 will be aggregated into a single record and inserted into B3.
- Since B3's default storage duration is 7 days, it will contain a maximum of 168 records per RF Domain after 7 days.
- Since B4's granularity is 1 day, every day 24 records from B3 will be aggregated into a single record and inserted into B4.
- Since B4's default storage duration is 365 days, it will contain a maximum of 365 records per RF Domain after 1 year.

Data Expiration:

The expiration of older records (also referred to as purging or deleting of records) occurs along with data aggregation for each bucket.

Let us consider (with default data storage-duration settings) the expiration of data for any one of the statistical buckets.

- As stated earlier, at the end of 8 hours B1 will have 960 records per RF Domain. After a period of 8 hours and 10 minutes, all 960 records are aggregated into 144 records and inserted into B2. To enable B1 to hold exactly 8 hours worth of data, 20 of the oldest records (corresponding to the first 10 minutes) are purged from B1 at the end of 8 hours and 10 minutes. This expiration cycle is triggered every 10 minutes.
- At the end of 24 hours B2 will have 144 records per RF Domain. After a period of 24 hours and 10 minutes, one of the oldest record (corresponding to the first 10 minutes) is purged from B2. This expiration cycle is triggered every 10 minutes to enable B2 to maintain exactly 24 hours worth of data.
- At the end of 7 days B3 will have 168 records per RF Domain. After a period of 7 days and one hour one of the oldest record (corresponding to the first hour) is purged from B3. This expiration cycle is triggered every 1 hour to enable B3 to maintain exactly 7 days worth of data.
- At the end of 365 days B4 will have 365 records per RF Domain. After 365 days, the oldest records (corresponding to the first day) are purged from B4. This expiration cycle is triggered every 1 day to enable B4 to maintain exactly 365 days worth of data.

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics
avc-update-interval 120

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics
update-interval 30

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics
wireless-clients-update-interval 600

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database statistics
max-apps-per-client 20

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#nsight database summary duration
12 30 200 500

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory |
include nsight
 use nsight-policy nsight-noc
 nsight database statistics update-interval 30
 nsight database statistics wireless-clients-update-interval 600
 nsight database summary duration 12 30 200 500
 nsight database statistics avc-update-interval 120
 nsight database statistics max-apps-per-mu 20
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands

no	Reverts the NSight database related parameters configured to default values

7.2.16 override-wlan

Device Config Commands

Configures WLAN's RF Domain level overrides

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
override-wlan <WLAN> [shutdown|ssid|vlan-pool|wep128|wpa-wpa2-psk]

override-wlan <WLAN> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}|
wpa-wpa2-psk <WORD>]

override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]|transmit-key <1-4>]
```

Parameters

- `override-wlan <WLAN> [shutdown|ssid <SSID>|vlan-pool <1-4094> {limit <0-8192>}| wpa-wpa2-psk <WORD>]`

<WLAN>	Specify the WLAN name. Configure the following WLAN parameters: SSID, VLAN pool, and WPA-WPA2 key.
shutdown	Shuts down the WLAN's (identified by the <WLAN> keyword) operations on all mapped radios
SSID <SSID>	Configures the WLAN's *Service Set Identifier* (SSID) • <SSID> – Specify an SSID ID.
vlan-pool <1-4094> {limit <0-8192>}	Configures a pool of VLANs for the selected WLAN • <1-4094> – Specifies a VLAN pool ID from 1 - 4094. • limit – Optional. Limits the number of users on this VLAN pool • <0-8192> – Specify the user limit from 0 - 8192. **Note:** The VLAN pool configuration overrides the VLAN configuration.
wpa-wpa2-psk <WORD>	Configures the WLAN WPA-WPA2 key or passphrase for the selected WLAN • <WORD> – Specify a WPA-WPA2 key or passphrase.

- `override-wlan <WLAN> wep128 [key <1-4> hex [0<WORD>|2 <WORD>]|transmit-key <1-4>]`

<WLAN>	Specify the WLAN name.
wep128 [key <1-4> hex [0<WORD>| 2 <WORD>]| transmit-key <1-4>	Configures the WEP128 key for this WLAN, and also enables key transmission *Wired Equivalent Privacy* (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi -Fi) standard. WEP 128 uses a 104 bit key, which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. This results in a level of security and privacy comparable to that of a wired LAN. Contd..

	• key <1-4> hex – Configures a hexadecimal key (clear text or encrypted) and specifies the key's index.
	  • 0 <WORD> – Configures a clear text key. Specify a 4 - 32 character pass key.
	  • 2 <WORD> – Configures an encrypted key. Specify a 4 - 32 character pass key.
	• transmit-key <1-4> – Enables transmission of key index. Specify the key index.
	Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without the required adapters need to use WEP keys manually configured as hexadecimal numbers.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#override-wlan test vlan-pool 8

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 location SanJose
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes RF Domain level WLAN overrides

7.2.17 remove-override

Device Config Commands

Removes device overrides in order to enable profile settings to take effect

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
remove-override <PARAMETERS>
```

Parameters

- `remove-override <PARAMETERS>`

remove-override <PARAMETERS>	Removes settings configured at the device level based on the parameters passed. The profile (applied to the device) settings take effect once the device-level overrides are removed.

Example

```
rfs4000-229D58(config-device-00-23-68-22-9D-58)#remove-override ?
  adopter-auto-provisioning-policy-lookup  Use centralized auto-provisioning
                                           policy when adopted by another
                                           controller
  adoption                                 Adoption configuration
  adoption-mode                            Configure the adoption mode for the
                                           access-points in this RF-Domain
  alias                                    Alias
  all                                      Remove all overrides for the device
  application-policy                       Application Policy configuration
  area                                     Reset name of area where the system
                                           is located
  arp                                      Address Resolution Protocol (ARP)
  auto-learn                               Auto learning
  autogen-uniqueid                         Autogenerate a unique id
  autoinstall                              Autoinstall settings
  bridge                                   Bridge group commands
  captive-portal                           Captive portal
  cdp                                      Cisco Discovery Protocol
  channel-list                             Configure a channel list to be
                                           advertised to wireless clients
  cluster                                  Cluster configuration
  configuration-persistence                Automatic write of startup
                                           configuration file
  contact                                  The contact
  controller                               WLAN controller configuration
  country-code                             The country of operation
  critical-resource                        Critical Resource
  crypto                                   Encryption related commands
  device-upgrade                           Device firmware upgrade
  dot1x                                    802.1X
  dpi                                      Deep-Packet-Inspection (Application
                                           Assurance)
  dscp-mapping                             IP DSCP to 802.1p priority mapping
                                           for untagged frames
  email-notification                       Email notification configuration
  enforce-version                          Check the firmware versions of
                                           devices before interoperating
  environmental-sensor                     Environmental Sensors Configuration
```

```
  events                                  System event messages
  export                                  Export a file
  file-sync                               File sync between controller and
                                          adoptees
  firewall                                Enable/Disable firewall
  floor                                   Reset name of floor where the
                                          system is located
  geo-coordinates                         Geo co-ordinates for this device
  global                                  Remove global overrides for the
                                          device but keeps per-interface
                                          overrides
  gre                                     GRE protocol
  interface                               Select an interface to configure
  ip                                      Internet Protocol (IP)
  ipv6                                    Internet Protocol version 6 (IPv6)
  l2tpv3                                  L2tpv3 protocol
  l3e-lite-table                          L3e lite Table
  led                                     LED on the device
  lldp                                    Link Layer Discovery Protocol
  location                                The location
  logging                                 Modify message logging facilities
  mac-address-table                       MAC Address Table
  mac-auth                                802.1X
  memory-profile                          Memory-profile
  mint                                    MiNT protocol
  mpact-server                            MPACT server configuration
  noc                                     Noc related configuration
  ntp                                     Configure NTP
  offline-duration                        Duration to mark adopted device as
                                          offline
  override-wlan                           Overrides for wlans
  power-config                            Configure power mode
  preferred-controller-group              Controller group this system will
                                          prefer for adoption
  preferred-tunnel-controller             Tunnel Controller Name this system
                                          will prefer for tunneling extended
                                          vlan traffic
  rf-domain-manager                       RF Domain Manager
  router                                  Dynamic routing
  routing-policy                          Policy Based Routing Configuration
  sensor-server                           AirDefense WIPS sensor server
                                          configuration
  spanning-tree                           Spanning tree
  timezone                                The timezone
  traffic-class-mapping                   IPv6 traffic-class to 802.1p
                                          priority mapping for untagged
                                          frames
  traffic-shape                           Traffic shaping
  trustpoint                              Assign a trustpoint to a service
  tunnel-controller                       Tunnel Controller group this
                                          controller belongs to
  use                                     Set setting to use
  vrrp                                    VRRP configuration

  service                                 Service Commands

rfs4000-229D58(config-device-00-23-68-22-9D-58)#
```

7.2.18 rsa-key

Device Config Commands

Assigns an SSH RSA key

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a requesting client to access resources, if properly configured. The RSA key pair must be generated on the client. The public portion of the key pair resides with the controller, service platform, or access point locally, while the private portion remains on a secure area of the client.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
rsa-key ssh <RSA-KEY-NAME>
```

Parameters

- `rsa-key ssh <RSA-KEY-NAME>`

rsa-key ssh <RSA-KEY-NAME>	Assigns RSA key to SSH • <RSA-KEY-NAME> – Specifies the RSA key name. The key should be installed using PKI commands in the enable mode.

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#rsa-key ssh rsa-key1

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location SanJose
 no contact
 country-code us
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes RSA key from service

7.2.19 sensor-server

Device Config Commands

Configures an AirDefense sensor server resource for client terminations and WIPS event logging. This is the server that supports WIPS events on behalf of the controller or service platform.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}
```

Parameters

- `sensor-server <1-3> ip <IP/HOSTNAME> {port [443|<1-65535>]}`

sensor-server <1-3>	Sets a numerical index to differentiate this AirDefense sensor server from other servers. A maximum of 3 (three) sensor server resources can be defined.
ip <IP/HOSTNAME>	Configures the AirDefense sensor server's IP address or hostname • <IP/HOSTNAME> – Specify the IP address.
port [443|<1-65535>]	Optional. Configures the port. The options are: • 443 – The default port used by the AirDefense server. This is the default setting. • <1-65535> – Manually sets the port number of the AirDefense server from 1 - 65535

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#sensor-server 1 ip 172.16.10.7

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location SanJose
 no contact
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes configured sensor server settings

7.2.20 timezone

Device Config Commands

Configures device's timezone

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
timezone <TIMEZONE>
```

Parameters

- `timezone <TIMEZONE>`

timezone <TIMEZONE>	Configures the device's timezone

Example

```
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#timezone Etc/UTC

rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#show context
ap71xx 00-04-96-4A-A7-08
 use profile default-ap71xx
 use rf-domain default
 hostname TechPubAP7131
 floor 5thfloor
 layout-coordinates 1.0 2.0
 license AP aplicenseley@1234 aplicensekey@123
 rsa-key ssh rsa-key1
 location SanJose
 no contact
 timezone Etc/UTC
 stats open-window 2 sample-interval 77 size 10
 country-code us
 sensor-server 1 ip 172.16.10.7
 channel-list 2.4GHz 1,2
 override-wlan test vlan-pool 8
 mac-name 00-04-96-4A-A7-08 5.8TestAP
 neighbor-info-interval 50
rfs7000-37FABE(config-device-00-04-96-4A-A7-08)#
```

Related Commands

no	Removes device's configured timezone

7.2.21 trustpoint (device-config-mode)

Device Config Commands

Assigns trustpoints to validate various services, such as HTTPS, RADIUS CA, RADIUS server, external LDAP server, etc.

For more information on digital certificates and certificate authorities, see *trustpoint (profile-config-mode)*.

NOTE: Certificates/trustpoints used in this command should be verifiable as existing on the device.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8232, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
trustpoint [cloud-client|cmp-auth-operator|https|radius-ca|radius-ca-ldaps|
radius-server|radius-server-ldaps] <TRUSTPOINT-NAME>
```

Parameters

```
• trustpoint [cloud-client|cmp-auth-operator|https|radius-ca|radius-ca-ldaps|
radius-server|radius-server-ldaps] <TRUSTPOINT-NAME>
```

trustpoint	Assigns trustpoints to validate various services. The assigned trustpoint is used as the CA for validating the services.
cloud-client	Assigns trustpoint to validate cloud client. The trustpoint should be existing and installed on the device. Use this option on cloud-enabled access points and cloud-adopted, to secure the communication between the cloud AP and cloud client. The trustpoint should be existing and installed on the AP. The cloud-enabled access points are AP7502, AP7522, AP7532, and AP7562. For local-controller adopted APs, this configuration is not required,
cmp-auth-operator	Assigns an existing trustpoint to validate CMP auth operator. Once validated, CMP is used to obtain and manage digital certificates in a PKI network. Digital certificates link identity information with a public key enclosed within the certificate, and are issued by the CA. Use this command to specify the CMP-assigned trustpoint. When specified, devices send a certificate request to the CMP supported CA server, and download the certificate directly from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire. **Note:** When configured, this cmp-auth-operator trustpoint setting overrides the profile-level configuration.
https	Assigns an existing trustpoint to validate HTTPS
radius-ca	Assigns an existing trustpoint to validate client certificates in EAP

radius-ca-ldaps	Assigns an existing trustpoint to validate external LDAP server
radius-server	Assigns an existing trustpoint to validate RADIUS server certificate
radius-server-ldaps	Assigns an existing trustpoint to RADIUS server certificate to validate LDAP server
<TRUSTPOINT-NAME>	The following keyword is common to all of the above parameters: • <TRUSTPOINT-NAME> – After selecting the service to validate, specify the trustpoint name (should be existing and stored on the device). **Note:** By default, the system assigns the default-trustpoint to validate the following: https, radius-server, and radius-server-ldaps.

Example

A device's default HTTPS, RADIUS, and CMP certificate/trustpoint configuration is as follows:

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory |
include trustpoint
 trustpoint https default-trustpoint
 no trustpoint radius-ca
 trustpoint radius-server default-trustpoint
 no trustpoint radius-ca-ldaps
 trustpoint radius-server-ldaps default-trustpoint
 no trustpoint cmp-auth-operator
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#trustpoint https test

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context include-factory |
include trustpoint
 trustpoint https test
 no trustpoint radius-ca
 trustpoint radius-server default-trustpoint
 no trustpoint radius-ca-ldaps
 trustpoint radius-server-ldaps default-trustpoint
 no trustpoint cmp-auth-operator
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

7.2.22 raid

Device Config Commands

Enables chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on a service platform

The NX95XX (NX9500 and NX9510) series service platforms include a single Intel MegaRAID controller (virtual drive) with RAID-1 mirroring support enabled. The online virtual drive supports up to two physical drives that could require hot spare substitution if a drive were to fail. The WiNG software allows you to manage the RAID controller event alarm and syslogs supporting the array hardware from the service platform user interface without rebooting the service platform BIOS.

Although RAID controller drive arrays are available only on the NX95XX series service platforms, they can be administrated on behalf of a NX95XX profile by a different model service platform or wireless controller.

Supported in the following platforms:

- Service Platforms — NX7530, NX9500, NX9510, NX9600

Syntax

```
raid alarm enable
```

Parameters

- `raid alarm enable`

alarm enable	Enables audible alarm, which is triggered a RAID drives fails. When triggered the alarm can be disabled by executing the *raid > silence* command in the device's Priv Exec mode.

Example

```
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#raid alarm enable

nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#show context
nx9000 B4-C7-99-6C-88-09
 use profile default-nx9000
 use rf-domain default
 hostname nx9500-6C8809
 ip default-gateway 192.168.13.2
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface vlan1
  ip address 192.168.13.13/24
 logging on
 logging console warnings
 logging buffered warnings
 raid alarm enable
nx9500-6C8809(config-device-B4-C7-99-6C-88-09)#
```

Related Commands

no	Disables RAID alarm

7.3 T5 Profile Config Commands

PROFILES

A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS wireless controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The *Customer Premises Equipment* (CPEs) are the T5 controller managed radio devices using the IPX operating system. These CPEs use a DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To navigate to this instance, use the following commands:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#?
T5 Profile Mode commands:
  cpe             T5 CPE configuration
  interface       Select an interface to configure
  ip              Internet Protocol (IP)
  no              Negate a command or set its defaults
  ntp             Configure NTP
  override-wlan   Configure RF Domain level overrides for wlan
  t5              T5 configuration
  t5-logging      Modify message logging facilities
  use             Set setting to use

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

<DEVICE>(config-profile-<PROFILE-NAME>)#
```

The following table summarizes T5 profile configuration mode commands:

Command	Description	Reference
cpe	Configures T5 CPE related settings (IP address range and VLAN)	*page 7-495*
interface	Configures the T5 controller's interfaces	*page 7-497*
ip	Configures the default gateway's IP address	*page 7-499*
no	Removes or reverts this T5 controller profile settings	*page 7-500*
ntp	Configures the NTP server associated with this T5 profile	*page 7-501*
override-wlan	Configures the RF Domain level overrides for applied on a WLAN on this T5 profile	*page 7-502*
t5	Configures the logged T5 controller's country of operation	*page 7-503*
t5-logging	Configures a maximum of 5 (five) remote hosts capable of receiving syslog messages from this selected T5 controller	*page 7-504*
use	Defines this T5 profile's management settings	*page 7-505*

7.3.1 cpe

T5 Profile Config Commands

Configures T5 CPE related settings. This command is available both in the T5 profile and T5 device contexts

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax T5 Profile & T5 Device Context

```
cpe [address led]

cpe address vlan <1-4094> <START-IP> <END-IP>

cpe led cpe <cpe1-24>

The following commands are specific to the T5 device context:

cpe [boot|reload|upgrade]

cpe boot system <cpe1-24> <primary|secondary>

cpe reload <cpe1-24>

cpe <cpe1-24> upgrade <IMAGE-LOCATION>
```

Parameters

- `cpe address vlan <1-4094> <START-IP> <END-IP>`

cpe address	Configures the range of addresses that can be assigned to adopted CPEs
vlan <1-4094>	Configures the VLAN assigned to the CPEs managed by this T5 controller
<START-IP> <END-IP>	Configures the range of IP addresses that can be assigned to the CPEs managed by this T5 controller • <START-IP> – Specify the first IP address in the range. • <END-IP> – Specify the last IP address in the range.

- `cpe led cpe <cpe1-24>`

cpe led	Enables flashing of LEDs on specified CPEs
cpe <cpe1-24>	Identifies the CPE(s) on which the operation is performed • <cpe1-24> – Configures the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, & 5 are adopted and ready, then enter this value as cpe1-5.

- `cpe boot system <cpe1-24> <primary|secondary>`

cpe boot system	Changes the image used by a CPE to boot. When reloading, the CPE uses the specified image.
<cpe1-24>	Identifies the CPE(s) on which the operation is performed • <cpe1-24> – Configures the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, & 5 are adopted and ready, then enter this value as cpe1-5.

<primary|secondary>	Select the next boot image • primary – Uses the primary image when reloading • secondary – Uses the secondary image when reloading

- `cpe reload <cpe1-24>`

cpe reload	Reloads all or specified CPEs.
<cpe1-24>	Identifies the CPE(s) to reload • <cpe1-24> – Configures the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, & 5 are adopted and ready, then enter this value as cpe1-5.

- `cpe <cpe1-24> upgrade <IMAGE-LOCATION>`

cpe <cpe1-24> upgrade <IMAGE-LOCATION>	Upgrades all or specified CPEs • <cpe1-24> – Identifies the CPE(s) to upgrade. Specify the CPE's ID from cpe1 - cpe24. To enable led flashing on all adopted CPEs, enter cpe1-X, where X is the total number of adopted CPEs. For example, if CPEs 1, 2, 3, 4, & 5 are adopted and ready, then enter this value as cpe1-5. • upgrade <IMAGE-LOCATION> – Uses the image specified here to upgrade identified CEPs. • <IMAGE-LOCATION> – Specify the firmware image location using one of the following options: path/file tftp://<IP>/path/file ftp://<user>:<passwd>@<IP>/path/file

Example

```
nx9500-6C8809(config-profile-T5TestProfile)#cpe address vlan 200 192.168.13.26
192.168.13.30

nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
 interface fe 5 2
.....................................................................
 interface radio 11 1
 interface fe 9 2
 interface radio 18 1
 interface fe 9 1
 use firewall-policy default
 service pm sys-restart
 cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
```

7.3.2 interface

T5 Profile Config Commands

Configures the T5 controller's interfaces

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
interface [<WORD>|dsl|fe|ge|radio|vlan]

interface [<WORD>|dsl <1-24>|fe <1-24> <1-2>|ge <1-2>|radio <1-24> <1-2>|vlan <1-4094>]
```

Parameters

```
• interface [<WORD>|dsl <1-24>|fe <1-24> <1-2>|ge <1-2>|radio <1-24> <1-2>|vlan <1-4094>]
```

<WORD>	Configures the interface identified by the <WORD> keyword
dsl <1-24>	Configures the specified DSL interface. A T5 controller uses the IPX operating system to manage its connected radio devices, as opposed to the WiNG operating used by controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs are the T5 controller managed radio devices using the IPX operating system. These CPEs use DSL as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack. • <1-24> – Specify the DSL port index from 1 - 24.
fe <1-24> <1-2>	Configures the specified FastEthernet interface. The T5 controller has the following FastEthernet port designations: fe1-fe2 (fe1-fe2 are for up to 24 CPE devices managed by a T5 controller). • <1-24> – Specify the DSL port index from 1 - 24. • <1-2> – Specify the FastEthernet interface to configure. In the FastEthernet interface configuration mode, specify the interface settings.
ge <1-2>	Configures the specified GigabitEthernet interface. T5 controllers have two Ethernet port designations, These are ge1 and ge2. The GE ports can be RJ-45 or fiber ports supporting 10/100/1000Mbps. • <1-2> – Specify the interface index from 1 - 2. In the GigabitEthernet interface configuration mode, specify the interface settings.
radio <1-24> <1-2>	Configures the specified radio interface. T5 controller managed CPE device radios can have their radio configurations overridden once their radios have successfully associated and have been provisioned by the adopting controller, service platform, or peer model AP controller access point. • <1-24> – Specify the radio interface index from 1 - 24. • <1-2> – Allows the second radio to be specified as a radio interface. For example, this is "interface radio X Y" where 'X' is the DSL line number and 'Y' is the radio interface (number).

vlan <1-4094>	Configures the specified VLAN interface. Once configured, the VLAN interface provides layer 3 (IP) T5 controller access or provides layer 3 service on a VLAN. The VLAN interface defines which IP address is associated with each VLAN ID a T5 controller is connected to. A VLAN interface is created for the default VLAN (VLAN 1) to enable remote administration. This interface is also used to map VLANs to IP4 and IPv6 formatted IP address ranges. This mapping determines the destination for routing. • <1-4094> – Specify the VLAN interface index from 1 - 4094. In the VLAN configuration mode, specify the interface's primary IP address in the A.B.C.D/M format. Optionally specify the secondary IP address.

Example

```
rfs7000-37FABE(config-profile-t5Profile)#interface dsl 1

rfs7000-37FABE(config-profile-t5Profile-if-dsl1)#?
Interface configuration commands:
  description       Port description
  ds-interleaver    Enable impulse noise protection in the downstream
                    direction
  ds-max-datarate   Configure maximum allowed downstream rate for the
                    interface
  ds-min-margin     Configure the minimum downstream signal-to-noise(SNR)
                    ratio margin
  ds-target-margin  Configure the desired downstream signal-to-noise (SNR)
                    ratio margin
  duplex            Set duplex to interface
  flowcontrol       Set flowcontrol to interface
  line-power        Use the line-power command to apply power to the interface
  no                Negate a command or set its defaults
  qos               QOS settings
  shutdown          Shutdown the selected interface
  speed             Configure speed
  switchport        Set switching mode characteristics
  us-interleaver    Enable impulse noise protection in the upstream direction
  us-max-datarate   Configure maximum allowed upstream rate for the interface
  us-min-margin     Configure the minimum upstream signal-to-noise (SNR) ratio
                    margin
  us-target-margin  Configure the desired upstream signal-to-noise (SNR) ratio
                    margin

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
  service           Service Commands
--More--
rfs7000-37FABE(config-profile-t5Profile-if-dsl1)#
```

Related Commands

no	Removes the selected interface configuration on the T5 device

7.3.3 ip

T5 Profile Config Commands

Configures the default gateway's IP address

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
ip default-gateway <IP>
```

Parameters

- `ip default-gateway <IP>`

ip default-gateway <IP>	Enter the default gateway's IP address in the A.B.C.D format.

Example

```
nx9500-6C8809(config-profile-t5Profile)#ip default-gateway 192.168.13.7

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
 interface fe 5 2
 interface ge 2
 interface ge 1
 interface fe 5 1
--More--
nx9500-6C8809(config-profile-t5Profile)#
```

7.3.4 no

T5 Profile Config Commands

Removes or reverts this T5 controller profile settings

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
no [cpe|interface|ntp|override-wlan|t5-logging|use]

no cpe led cpe <1-24>

no interface vlan <2-4094>

no ntp server <IP>

no override-wlan <WLAN-NAME> vlan

no t5-logging host <IP>

no use management-policy
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts to default the selected T5 profile's or device's settings

Example

```
nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
.................................................
 use firewall-policy default
 ntp server 192.168.13.2
 service pm sys-restart
nx9500-6C8809(config-profile-t5Profile)#

nx9500-6C8809(config-profile-t5Profile)#no ntp server 192.168.13.2

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
.................................................
 use firewall-policy default
 service pm sys-restart
nx9500-6C8809(config-profile-t5Profile)#
```

7.3.5 ntp

T5 Profile Config Commands

Configures the NTP server associated with this T5 profile. T5 controllers, using this profile, will obtain their system time from the specified NTP server resources.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
ntp server <IP>
```

Parameters

```
• ntp server <IP>
```

ntp server <IP>	Specify the NTP server's IP address. You can specify a maximum of 3 (three) NTP server resources.

Example

```
nx9500-6C8809(config-profile-t5Profile)#ntp server 192.168.13.2

nx9500-6C8809(config-profile-t5Profile)#show context
profile t5 t5Profile
 ip default-gateway 192.168.13.7
 no autoinstall configuration
 no autoinstall firmware
 interface dsl 5
 ..................................................
 use firewall-policy default
 ntp server 192.168.13.2
 service pm sys-restart
nx9500-6C8809(config-profile-t5Profile)#
```

Related Commands

no	Removes the NTP server's IP address

7.3.6 override-wlan

T5 Profile Config Commands

Use this option to configure RF Domain level configuration for WLAN. The override configured here are applied to all T5 devices using this T5 profile.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
override-wlan <WLAN-NAME> vlan <1-4094>
```

Parameters

- `override-wlan <WLAN-NAME> vlan <1-4094>`

override-wlan <WLAN-NAME>	Overrides the specified WLAN's VLAN configuration <WLAN-NAME> – Specify the WLAN's name.
vlan <1-4094>	Specify the new VLAN option • <1-4094> – Specify the VLAN from 1 - 4094.

Example

The following example displays the WLAN SJOffWLan configuration:

```
nx9500-6C8809(config-wlan-SJOffWLan)#show context
wlan SJOffWLan
 description "SJ Office WLAN"
 ssid SJOffWLan
 vlan 468
 bridging-mode local
 encryption-type ccmp
 authentication-type eap-psk
 use aaa-policy test
nx9500-6C8809(config-wlan-SJOffWLan)#
```

The following example overrides the SJOffWLan WLAN's VLAN configuration on the T5 profile:

```
nx9500-6C8809(config-profile-testT5)#override-wlan SJOffWLan vlan 30

nx9500-6C8809(config-profile-testT5)#show context include-factory | include
override-wlan
 override-wlan SJOffWLan vlan 30
nx9500-6C8809(config-profile-testT5)#
```

Related Commands

no	Removes the RF Domain level overrides for applied on a WLAN on this T5 profile

7.3.7 t5

T5 Profile Config Commands

Configures this T5 controller's country of operation

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
t5 country-code <WORD>
```

Parameters

- `t5 country-code <WORD>`

country-code <WORD>	Configures the 2 letter ISO-3166 country code for this T5 controller

Example

```
nx9500-6C8809(config-profile-T5TestProfile)#t5 country-code us

nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
 no autoinstall configuration
 no autoinstall firmware
 interface vlan1
 interface vlan4090
 interface fe 5 2
.....................................................................
 interface fe 9 1
 use firewall-policy default
 service pm sys-restart
 t5 country-code US
 cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
```

7.3.8 t5-logging

T5 Profile Config Commands

Configures a maximum of 5 (five) remote hosts capable of receiving syslog messages from this selected T5 controller

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
t5-logging host <IP> severity [error|info|notice|trace|warning] facility
[local0|local1|local2|local3|local4|local5|local6|local7]
```

Parameters

```
• t5-logging host <IP> severity [error|info|notice|trace|warning] facility
[local0|local1|local2|local3|local4|local5|local6|local7]
```

t5-logging host <IP>	Configures syslog message logging settings • host <IP> – Configures the external syslog remote host resource's IP address. This is the host dedicated to receive T5 syslog messages.
severity [error|info|notice|trace|warning]	Configures the syslog message filtering severity level. The options are: • Error – Only forwards error and above syslog event messages. • Info – Only forwards informational and above syslog event messages. • notice – Only forwards syslog notices relating to general device operational events. These are events that are of more interest than the "info" events. • trace – Only forwards trace routing event messages • warning – Only forwards warnings and above syslog event messages
facility [local0|local1|local2|local3|local4|local5|local6|local7]	Configures the facility level for log messages sent to the syslog server. The facility level specifies the type of program logging the message. Specifying the facility level allows the configuration file to specify that message handling will vary with varying facility type. The options are: local0, local1, local2, local3, local4, local5, local5, local6, local7. The default value is local7.

Example

```
nx9500-6C8809(config-profile-T5TestProfile)#t5-logging host 192.168.13.10
severity warning facility local6

nx9500-6C8809(config-profile-T5TestProfile)#show context
profile t5 T5TestProfile
 t5-logging host 192.168.13.10 severity warning facility local6
 no autoinstall configuration
.....................................................................
 no autoinstall firmware
 t5 country-code US
 cpe address vlan 200 192.168.13.26 192.168.13.30
nx9500-6C8809(config-profile-T5TestProfile)#
```

Related Commands

no	Modifies message logging severity level and facilities

7.3.9 use

T5 Profile Config Commands

Associates a management policy with this T5 profile. The specified policy is applied to all T5 controllers using this profile.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
use management-policy <POLICY-NAME>
```

Parameters

- `use management-policy <POLICY-NAME>`

use management-policy <POLICY-NAME>	Associates a management policy with this T5 profile (should be existing and configured) • <POLICY-NAME> – Specify the management policy's name.

Example

```
nx9500-6C8809(config-profile-t5Profile)#use management-policy default
Trustpoints HTTPS Server  and RSA keys for SSH can be configured with 'trustpoint'
and 'rsa-key' commands in device context
nx9500-6C8809(config-profile-t5Profile)#
```

Related Commands

no	Removes the management policy used with this T5 profile

7.4 EX3524 & EX3548 Profile/Device Config Commands

PROFILES

Creates a new EX3524 and EX3548 profile and enters its configuration mode.

To navigate to this instance, use the following commands:

```
<DEVICE>(config)#profile ex35xx <EX35XX-PROFILE-NAME>
```

Where ex35xx can be a EX3524 or a EX3548 device type.

```
<DEVICE>(config-profile-<EX35XX-PROFILE-NAME>)#?
EX35XX Profile Mode commands:
  interface  Select an interface to configure
  ip         Internet Protocol (IP)
  no         Negate a command or set its defaults
  power      EX3500 Power over Ethernet Command
  upgrade    Configures upgrade option for ex3500 system
  use        Set setting to use

  clrscr     Clears the display screen
  commit     Commit all changes made in this session
  do         Run commands from Exec mode
  end        End current mode and change to EXEC mode
  exit       End current mode and down to previous mode
  help       Description of the interactive help system
  revert     Revert changes
  service    Service Commands
  show       Show running system information
  write      Write running configuration to memory or terminal

<DEVICE>(config-profile-<EX35XX-PROFILE-NAME>)#
```

The following table summarizes EX3524 and EX3548 profile/device configuration mode commands:

Command	Description	Reference
interface	Selects an interface type and enters the selected interface's configuration mode	*page 7-507*
ip	Configures the default gateway through which this EX35XX switch can reach other subnets	*page 7-527*
power	Enables power inline compatibility mode on this EX35XX profile	*page 7-528*
upgrade	Configures adopted EX35XX switch upgrade settings	*page 7-529*
use	Applies an EX3500 management policy to this EX35XX profile	*page 7-530*
no	Removes or reverts this EX35XX profile's settings	*page 7-531*

7.4.1 interface

EX3524 & EX3548 Profile/Device Config Commands

This command selects an interface type and enters the selected interface's configuration mode. The EX35XX switch has GE and VLAN interfaces. Select the interface type and provide the interface ID to enter its configuration mode.

Command	Description	Reference
interface	Selects an interface type and enters the selected interface's configuration mode	*page 7-508*
interface-ge-config commands	Summarizes GE interface configuration mode commands	*page 7-510*
interface-vlan-config commands	Summarizes VLAN interface configuration mode commands	*page 7-523*

7.4.1.1 interface

interface

Selects the EX35XX interface type and enters the selected interface's configuration mode

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
interface [ge 1 <1-48>|vlan <1-4094>]
```

Parameters

- `interface [ge 1 <1-48>|vlan <1-4094>]`

interface	Selects the EX35XX interface type and enters its configuration mode. The interface options available are: GE and VLAN
ge 1 <1-48>	Selects a GE interface to configure • 1 – Configures the GE interface unit identifier as 1 • <1-48> – Configures the physical port number from 1 - 24/48 **Note:** For the EX3524 model switch the GE port range is 1-24, and for the EX3548 it is 1-48.
vlan <1-4094>	Selects a VLAN interface to configure • <1-4094> – Specify the VLAN interface ID from 1 - 4094.

Example

```
nx4500-5CFA8E(config-profile-testEX35XX)#interface vlan 1
nx4500-5CFA8E(config-profile-testEX35XX-if-vlan1)#?
 commands:
  ip        Internet Protocol (IP)
  no        Negate a command or set its defaults

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

nx4500-5CFA8E(config-profile-testEX35XX-if-vlan1)#

nx4500-5CFA8E(config-profile-testEX35XX)#interface ge 1 1
nx4500-5CFA8E(config-profile-testEX35XX-if-ge1-1)#?
 commands:
  access-group  Access group to bind a port to an ACL name
  no            Negate a command or set its defaults
  port          Configures the characteristics of the port
  power         EX3500 Power over Ethernet Command
  shutdown      Shutdown the selected interface
  speed-duplex  Configures speed and duplex operation
  switchport    Configures switch mode characteristics
  use           Set setting to use
```

```
  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

nx4500-5CFA8E(config-profile-testEX35XX-if-ge1-1)#
```

Related Commands

no	Removes this interface (GE/VLAN) settings from the EX35XX profile or device
interface-ge-config commands	Summarizes GE interface configuration mode commands
interface-vlan-config commands	Summarizes VLAN interface configuration mode commands

7.4.1.2 interface-ge-config commands

interface

The following table lists the EX35XX GE interface configuration mode commands:

Command	Description	Reference
access-group	Binds an EX3500 ACL to the selected port	*page 7-511*
port	Enables port monitoring on the selected port	*page 7-512*
power	Turns power on or off for the selected port	*page 7-514*
shutdown	Shuts down the selected port	*page 7-516*
speed-duplex	Configures the speed and duplex mode of the selected port when auto-negotiation is disabled. Auto-negotiation is enabled by default.	*page 7-517*
switch-port	Configures the switch mode characteristics of the selected port	*page 7-518*
use	Applies a EX3500 QoS policy map with the selected port	*page 7-520*
no	Removes or reverts the selected port's settings	*page 7-521*

7.4.1.2.1 access-group

interface-ge-config commands

Binds an EX3500 ACL to the selected port

When applied to the port, the ACL takes effect. Only one ACL can be bound to a port at a time. In case you bind a new ACL to a port with an existing ACL binding, the old binding is replaced with the new one.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list]
<ACL-NAME> in {time-range <TIME-RANGE-NAME>}
```

Parameters

```
• access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list]
<ACL-NAME> in {time-range <TIME-RANGE-NAME>}
```

access-group	Binds a EX3500 ACL with this GE port. Select ACL type and specify the ACL name. The ACL should be existing and configured.
ex3500-ext-access-list <ACL-NAME>	Binds an existing and configured EX3500 extended ACL • <ACL-NAME> – Specify the ACL name.
ex3500-std-access-list <ACL-NAME>	Binds an existing and configured EX3500 standard ACL • <ACL-NAME> – Specify the ACL name.
mac-access-list <ACL-NAME>	Binds an existing and configured EX3500 MAC ACL • <ACL-NAME> – Specify the MAC ACL name.
in	Applies the specified ACL to all incoming packets
time-range <TIME-RANGE-NAME>	Optional. Associates a EX3500 absolute or periodic time range with this access group. The specified ACL is bound to the port during the time period specified by the associated time range. • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured).

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#access-group ex3500-ext-
access-list EX3500_ACL_EXT_1 in time-range EX3500_TimeRange_01

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Removes the GE port EX3500 ACL binding

7.4.1.2.2 port

interface-ge-config commands

Enables port monitoring on the selected port. This allows the port to monitor specified ports and/or MAC address(es). When enabled, the switch sends a copy of the network packets seen on the specified switch port (or VLAN interface) to the monitoring switch port. These packets are analyzed and debugged to provide vital information, such as network performance, intrusion alerts, etc.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
port monitor [ethernet|ex3500-ext-access-list|ex3500-std-access-list|mac-access-list|mac-address|vlan]

port monitor ethernet 1 <1-52> {both|rx|tx}

port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME>

port monitor mac-address <MAC>

port monitor vlan <1-4094>
```

Parameters

- `port monitor ethernet 1 <1-52> {both|rx|tx}`

port monitor ethernet 1 <1-52>	Configures the characteristics of this GE port
	• monitor – Enables monitoring of another port
	  • ethernet 1 – Selects Ethernet interface and configures the port identifier as 1
	  • <1-52> – Configures the Ethernet unit number from 1 - 52

{both|rx|tx}	After specifying the port, optionally configure the following: • both – Optional. Monitors both incoming and outgoing traffic • rx – Optional. Monitors only incoming traffic • tx – Optional. Monitors only outgoing traffic

- `port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME>`

port monitor	Configures the characteristics of this GE port • monitor – Enables monitoring of another port
[ex3500-ext-access-list|ex3500-std-access-list|mac-access-list] <ACL-NAME>	After specifying the port, apply one of the following ACLs: • ex3500-ext-access-list – Applies a EX3500 extended ACL • ex3500-std-access-list – Applies a EX3500 standard ACL • mac-access-list – Applies a MAC ACL with EX3500 deny or permit rules • <ACL-NAME> – Specify the ACL name (should be existing and configured).

- `port monitor mac-address <MAC>`

port monitor	Configures the characteristics of this GE port • monitor – Enables monitoring of another port

mac-address <MAC>	Configures the MAC address to monitor • <MAC> – Specify the MAC address in the AA-BB-CC-DD-EE-FF format.

- `port monitor vlan <1-4094>`

port monitor	Configures the characteristics of this GE port • monitor – Enables monitoring of another port
vlan <1-4094>	Configures the VLAN interface to monitor • <1-4094> – Specify the VLAN ID from 1 - 4094.

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#port monitor vlan 20

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Disables port monitoring on the selected port and removes the settings

7.4.1.2.3 power

interface-ge-config commands

Enables power allocation to the selected port. When enabled, the power is allocated to this port. Use the command to configure the power allocation settings, such as maximum power allocated, priority level of this port in connection with power allocation, and the time range within which these power settings are applied.

This option is enabled by default.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
power inline {maximum|priority|time-range}
power inline {maximum allocation milliwatts <3000-34200>}
power inline {priority [critical|high|low]}
power inline {time-range <TIME-RANGE-NAME>}
```

Parameters

- `power inline {maximum allocation milliwatts <3000-34200>}`

power inline	Turns power on or off for the selected port. This option is enabled by default.
maximum allocation milliwatts <3000-34200>	Optional. Configures the maximum power allocation, in milliwatts, for this port • <3000-34200> – Specify a value from 3000 - 34200 milliwatts. The default is 34200 milliwatts.

- `power inline {priority [critical|high|low]}`

power inline	Turns power on or off for the selected port. This option is enabled by default.
priority [critical|high|low]	Optional. Configures the PoE power priority as: • critical – Configures the PoE power priority as critical • high – Configures the PoE power priority as high • low - Configures the PoE power priority as low (this is the default setting)

- `power inline {time-range <TIME-RANGE-NAME>}`

power inline	Turns power on or off for the selected port. This option is enabled by default.
time-range <TIME-RANGE-NAME>	Optional. Binds a EX3500 time range to this port • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured).

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline maximum
allocation milliwatts 30000

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline priority critical

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#power inline time-range
EX3500_TimeRange_01

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Disables power allocation to the selected port

7.4.1.2.4 shutdown

interface-ge-config commands

Shuts down the selected port

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
shutdown
```

Parameters

None

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#shutdown

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  shutdown
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Brings up a shutdown port

7.4.1.2.5 speed-duplex

interface-ge-config commands

Configures the speed and duplex mode of the selected port when auto-negotiation is disabled. Auto-negotiation is enabled by default.

This option is disabled by default.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
speed-duplex [100full|100half|10full|10half]
```

Parameters

- `speed-duplex [100full|100half|10full|10half]`

speed-duplex [100full|100half| 10full|10half]	Configures the speed and duplex mode of the selected port to one of the following modes: • 100full – Forces 100 Mbps full-duplex operation • 100half – Forces 100 Mbps half-duplex operation • 10full – Force 10 Mbps full-duplex operation • 10half – Force 10 Mbps half-duplex operation When configured, forces the switch to operate at the specified speed and mode.

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#speed-duplex 100half

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  shutdown
  speed-duplex 100half
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Removes the speed and duplex settings configured for this EX35XX profile

7.4.1.2.6 switch-port

interface-ge-config commands

Configures the switch mode characteristics of the selected port

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
switchport [allowed|l2protocol-tunnel|mode|native]

switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>]

switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]

switchport mode [access|hybrid|trunk]

switchport native
```

Parameters

- `switchport allowed [add <VLAN-ID>|none|remove <VLAN-ID>]`

switchport allowed [add <VLAN-ID>| none| remove <VLAN-ID>]	Configures VLAN groups on the selected interface.
	• add <VLAN-ID> – Configures the list of VLAN identifiers to add. When the add option is used, the interface is assigned to the specified VLANs, and membership in all previous VLANs is retained.
	  • <VLAN-ID> – Specify the list of VLANs to add.
	• none – Removes all VLANs from the current list
	• remove <VLAN-ID> – Configures the list of VLAN identifiers to remove. When the remove option is used, the specified VLANs are removed from the current list.
	  • <VLAN-ID> – Specify the list of VLANs to remove.

- `switchport l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]`

switchport l2protocol-tunnel [cdp|lldp|pvst+| spanning-tree|vtp]	Enables *layer 2 protocol tunneling* (L2PT) for the specified protocol. Specify the protocol: • cdp – Cisco Discovery Protocol • lldp – Link Layer Discovery Protocol • pvst+ – Cisco Per VLAN Spanning Tree Plus • spanning-tree – Spanning Tree (STP, RSTP, MSTP) • vtp – Cisco VLAN Trunking Protocol L2PT is disabled for all of the above specified protocols by default.

- `switchport mode [access|hybrid|trunk]`

switchport mode [access|hybrid| trunk]	Configures the VLAN membership mode for this port • access – The port is configured as an access VLAN interface. It transmits and receives packets untagged frames on a single VLAN. Contd..

	• trunk – Configures the selected port as an end-point for a VLAN trunk. A trunk link is configured between two switches, and it carries frames on more than one VLANs. These frames are tagged in order to identify the source VLAN. Frames belonging to the port's default VLAN are also transmitted as tagged frames. • hybrid – Configures the selected port as a hybrid VLAN interface. When configured as hybrid, the port can transmit either tagged or untagged frames. This is the default setting.

- `switchport native vlan <1-4094>`

switchport native vlan <1-4094> in	Configures the VLAN membership mode for this port • native vlan <1-4094> – Configures the *port's VLAN ID* (PVID) (this is the port's default VLAN ID). Frames from the specified VLAN ingress untagged at this port. The default value is 1. When using *access* mode, and an interface is assigned to a new VLAN, the *port's VLAN ID* (PVID) is automatically set to the identifier for that VLAN. When using *hybrid* mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#switchport mode access

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  shutdown
  speed-duplex 100half
  switchport mode access
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Removes the selected port's switchport characteristics

7.4.1.2.7 use

interface-ge-config commands

Applies a EX3500 QoS policy map with the selected port

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in
```

Parameters

- `use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME> in`

use ex3500-policy-map <EX3500-QoS-POLICY-MAP-NAME>	Applies a EX3500 QoS policy map with the selected port • <EX3500-QoS-POLICY-MAP-NAME> – Specify the EX3500 QoS policy map name (should be existing and configured) • in – Applies the specified policy to traffic ingressing at the selected port.

Example

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#use ex3500-policy-map in test

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  shutdown
  speed-duplex 100half
  switchport mode access
  use ex3500-policy-map in test
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

Related Commands

no	Disassociates the EX3500 QoS policy map linked to this EX3500 profile

7.4.1.2.8 no

interface-ge-config commands

Removes or reverts the selected port's settings

Supported in the following platforms:

- Switches — EX3524, EX3548

Syntax

```
no [access-group|port|power|shutdown|speed-duplex|switchport|use]

no access-group [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list]
<ACL-NAME> in

no port monitor [ethernet|ex3500-ext-access-list|ex3500-std-access-list|mac-
access-list|mac-address|vlan]

no port monitor ethernet 1 <1-52>

no port monitor [ex3500-ext-access-list|ex3500-std-access-list|mac-access-list]
<ACL-NAME>

no port monitor mac-address <MAC>

no port monitor vlan <1-4094>

no power inline {maximum allocation|priority|time-range}

no shutdown

no speed-duplex

no switchport [l2protocol-tunnel [cdp|lldp|pvst+|spanning-tree|vtp]|native vlan]

no use ex3500-policy-map in
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts the selected port's settings based on the parameters passed

Example

The following example shows the EX3524 profile's GE port 20's settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  shutdown
  speed-duplex 100half
  switchport mode access
  use ex3500-policy-map in test
  power inline maximum allocation milliwatts 30000
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#

nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no shutdown
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no power inline maximum
allocation
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#no use ex3500-policy-map in
```

The following example shows the EX3524 profile's GE port 20's settings after the 'no' commands are executed:

```
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#show context
 interface ge 1 20
  speed-duplex 100half
  switchport mode access
  power inline maximum allocation milliwatts 32400
  power inline priority critical
  power inline time-range EX3500_TimeRange_01
  access-group ex3500-ext-access-list EX3500_ACL_EXT_1 in time-range
EX3500_TimeRange_01
  port monitor vlan 20
nx9500-6C8809(config-profile-testEX3524-if-ge1-20)#
```

7.4.1.3 interface-vlan-config commands

interface

The following table lists the VLAN interface configuration mode commands:

Command	Description	Reference
ip	Configures IP related settings for this VLAN interface	*page 7-524*
no	Removes the IP related settings configured for this VLAN interface	*page 7-526*

7.4.1.3.1 ip

interface-vlan-config commands

Configures IP related settings for this VLAN interface

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
ip address [<IP/M>|bootp|dhcp]

ip address <IP/M> {default-gateway <IP>|secondary <IP>}

ip address [bootp|dhcp]
```

Parameters

- `ip address <IP/M> {default-gateway <IP>|secondary <IP>}`

ip address <IP/M> {default-gateway <IP>|secondary <IP>}	Manually configures the selected VLAN interface's primary and secondary IPv4 addresses. It also allows to optionally configure the default gateway. • <IP/M> – Manually configures this VLAN interface's IP address in the A.B.C.D/M format. Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask can be either in the traditional format xxx.xxx.xxx.xxx or use classless format with the range /5 to /32. For example the subnet 255.255.224.0 would be /19. • default-gateway <IP> – Optional. Configures the default gateway's IP address. This is the gateway through which this switch can reach other subnets not found in the local routing table. Before specifying the default gateway, ensure that the network interface directly connecting to the gateway is configured on the route. By default no gateway is specified. • <IP> – Specify the IP address in the A.B.C.D address. • secondary <IP> – Optional. Configures this VLAN interface's secondary IP address • <IP> – Specify the secondary IP address in the A.B.C.D address

- `ip address [bootp|dhcp]`

ip address [bootp|dhcp]	Enables a DHCP or Bootp server to provide the primary IPv4 address for the selected VLAN interface • bootp – Enables the VLAN interface to get its IP address from a Bootp server • dhcp – Enables the VLAN interface to get its IP address from a DHCP server If selecting DHCP/Bootp, ensure that a server on the network has been configured to provide the necessary configuration to the switch. Using DHCP or Bootp results in frequent connectivity loss between the browser interface and the switch. Further, DHCP and Bootp cannot configure secondary IP addresses needed for multinetting.

Example

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#ip address 192.168.13.28/24
default-gateway 192.168.13.13

nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
 interface vlan 20
  ip address 192.168.13.28/24 default-gateway 192.168.13.13
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

Related Commands

no	Removes the IP address configured for this VLAN interface

7.4.1.3.2 no

interface-vlan-config commands

Removes the IP related settings configured for this VLAN interface

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
no ip address [<IP/M>|bootp|dhcp]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes this EX3500's selected VLAN's settings based on the parameters passed

Example

The following example shows the interface VLAN 20 setting before the 'no' command is executed:

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
 interface vlan 20
  ip address 192.168.13.28/24 default-gateway 192.168.13.13
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#

nx9500-6C8809(config-profile-testEX3524-if-vlan20)#no ip address 192.168.13.28/24
```

The following example shows the interface VLAN 20 setting after the 'no' command is executed:

```
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#show context
 interface vlan 20
nx9500-6C8809(config-profile-testEX3524-if-vlan20)#
```

7.4.2 ip

EX3524 & EX3548 Profile/Device Config Commands

Configures the default gateway through which this EX35XX switch can reach other subnets

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
ip default-gateway <IP>
```

Parameters

- `ip default-gateway <IP>`

ip default-gateway <IP>	Configures the default gateway's IP address in the A.B.C.D format • <IP> – Specify the IP address.

Example

```
nx9500-6C8809(config-profile-testEX3524)#ip default-gateway 192.168.13.13

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 no autoinstall configuration
 no autoinstall firmware
 interface ge 1 17
 interface ge 1 16
 interface ge 1 15
 interface ge 1 14
 interface ge 1 13
 interface ge 1 12
 interface ge 1 11
--More--
 interface ge 1 21
 use firewall-policy default
 service pm sys-restart
nx9500-6C8809(config-profile-testEX3524)#
```

7.4.3 power

EX3524 & EX3548 Profile/Device Config Commands

Enables power inline compatibility mode on this EX35XX profile. This option is disabled by default.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers – RFS4000, RFS6000, RFS7000
- Service Platforms – NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
power inline compatible
```

Parameters

- `power inline compatible`

power inline compatible	Enables power inline compatibility mode

Example

```
nx9500-6C8809(config-profile-testEX3524)#power inline compatible

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
 no autoinstall configuration
 no autoinstall firmware
 interface ge 1 17
 interface ge 1 16
 interface ge 1 15
 interface ge 1 14
 interface ge 1 13
 interface ge 1 12
 --More--
nx9500-6C8809(config-profile-testEX3524)#
```

7.4.4 upgrade

EX3524 & EX3548 Profile/Device Config Commands

Configures adopted EX35XX switch upgrade settings

For a EX35XX switch to adopt to and be managed by a WiNG controller, you need to upload two images on the switch. An *operation code* (opcode) image and an adopted image. The opcode image functions as an operating system that enables the WiNG controller to communicate with the EX35XX switch. This command allows you to configure the EX35XX's opcode image upgrade settings.

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
upgrade opcode [auto|path <LINE>|reload]
```

Parameters

- `upgrade opcode [auto|path <LINE>|reload]`

upgrade opcode	Configures the opcode image upgrade settings
auto	Enables automatic upgrade
path <LINE>	Configures the location of the opcode image
reload	Enables automatic reload after successful loading of the opcode image

Example

```
<EX35XX-DEVICE>#show versions
Unit 1
Serial Number          : 14136520900352
Hardware Version       : R01
EPLD Version           : 0.00
Number of Ports        : 28
Main Power Status      : Up
Role                   : Master
Loader Version         : 5.0.0.1-01A
Linux Kernel Version   : 2.6.22.18
Boot ROM Version       : 0.0.0.1
Operation Code Version : 5.0.0.0-03D
Adoptd Version         : 5.8.3.0-024D
<EX35XX-DEVICE>#

nx9500-6C8809(config-profile-testEX3524)#upgrade auto
nx9500-6C8809(config-profile-testEX3524)#upgrade reload
nx9500-6C8809(config-profile-testEX3524)#upgrade opcode path ftp://
anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
.........................................
 use firewall-policy default
 service pm sys-restart
 upgrade opcode auto
 upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
 upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#
```

7.4.5 use

EX3524 & EX3548 Profile/Device Config Commands

Applies an EX3500 management policy to this EX35XX profile

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
use ex3500-management-policy <POLICY-NAME>
```

Parameters

- `use ex3500-management-policy <POLICY-NAME>`

use ex3500-management-policy <POLICY-NAME>	Applies an EX3500 management policy to this EX35XX profile • <POLICY-NAME> – Specify the EX3500 management policy name (should be existing and configured).

Example

```
nx9500-6C8809(config-profile-testEX3524)#use ex3500-management-policy test
Trustpoints HTTPS Server and RSA keys for SSH can be configured with 'trustpoint'
and 'rsa-key' commands in device context
nx9500-6C8809(config-profile-testEX3524)#

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
 no autoinstall configuration
 no autoinstall firmware
 interface ge 1 17
 interface ge 1 16
 interface ge 1 15
 --More--
 use ex3500-management-policy test
 use firewall-policy default
 service pm sys-restart
 upgrade opcode auto
 upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
 upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#
```

7.4.6 no

EX3524 & EX3548 Profile/Device Config Commands

Removes or reverts this EX3500 profile's settings

Supported in the following platforms:

- Switches — EX3524, EX3548
- Wireless Controllers — RFS4000, RFS6000, RFS7000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600

Syntax

```
no [interface vlan <1-4094>|default-gateway {<IP>}|power inline compatible|
upgrade opcode [auto|path|reload]|use ex3500-management-policy]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts this EX3500 profile settings based on the parameters passed

Example

```
nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
 no autoinstall configuration
 no autoinstall firmware
 interface ge 1 17
 interface ge 1 16
 interface ge 1 15
 interface ge 1 14
 interface ge 1 13
 interface ge 1 12
 interface ge 1 11
 interface ge 1 10
 interface ge 1 24
 interface ge 1 22
 interface vlan 20
 interface ge 1 23
--More--
 use ex3500-management-policy test
 use firewall-policy default
 service pm sys-restart
 upgrade opcode auto
 upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
 upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#

nx9500-6C8809(config-profile-testEX3524)#no use ex3500-management-policy
nx9500-6C8809(config-profile-testEX3524)#no upgrade opcode reload
nx9500-6C8809(config-profile-testEX3524)#no interface vlan 20

nx9500-6C8809(config-profile-testEX3524)#show context
profile ex3524 testEX3524
 ip default-gateway 192.168.13.13
 power inline compatible
 no autoinstall configuration
--More--
 use firewall-policy default
 service pm sys-restart
 upgrade opcode auto
 upgrade opcode path ftp://anonymous:anonymous@192.168.13.10/ex35xx/EX3524.img
nx9500-6C8809(config-profile-testEX3524)#
```

8 AAA-POLICY

This chapter summarizes the *Authentication, Authorization, and Accounting (*AAA) policy commands in the CLI command structure.

A AAA policy enables administrators to define access control settings governing network permissions. External RADIUS and LDAP servers (AAA servers) also provide user database information and user authentication data. Each WLAN maintains its own unique AAA configuration.

AAA provides a modular way of performing the following services:

Authentication — Provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating *attribute-value* (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

Accounting — Collects and sends security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored locally on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it is applied equally to all interfaces on the access servers.

Use the (config) instance to configure AAA policy commands. To navigate to the config-aaa-policy instance, use the following commands:

```
<DEVICE>(config)#aaa-policy <POLICY-NAME>

rfs6000-37FABE(config)#aaa-policy test

rfs6000-37FABE(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting           Configure accounting parameters
  attribute            Configure RADIUS attributes in access and accounting
                       requests
  authentication       Configure authentication parameters
  health-check         Configure server health-check parameters
  mac-address-format   Configure the format in which the MAC address must be
                       filled in the Radius-Request frames
  no                   Negate a command or set its defaults
  proxy-attribute      Configure radius attribute behavior when proxying
                       through controller or rf-domain-manager
  server-pooling-mode  Configure the method of selecting a server from the
```

```
                        pool of configured AAA servers
  use                   Set setting to use

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-aaa-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

8.1 aaa-policy

- *AAA-POLICY*

The following table summarizes AAA policy configuration commands:

Table 8.1 *AAA-Policy-Config Commands*

Command	Description	Reference
accounting	Configures accounting parameters	*page 8-4*
attribute	Configure RADIUS attributes in access and accounting requests	*page 8-8*
authentication	Configures authentication parameters	*page 8-11*
health-check	Configures health check parameters	*page 8-16*
mac-address-format	Configures the MAC address format	*page 8-17*
no	Negates a command or sets its default	*page 8-19*
proxy-attribute	Configures the RADIUS server's attribute behavior when proxying through the wireless controller or the RF Domain manager	*page 8-21*
server-pooling-mode	Defines the method for selecting a server from the pool of configured AAA servers	*page 8-22*
use	Defines the AAA command settings	*page 8-23*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

8.1.1 accounting

aaa-policy

Configures the server type and interval at which interim accounting updates are sent to the server. A maximum of 6 accounting servers can be configured.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
accounting [interim|server|type]

accounting interim interval <60-3600>

accounting server [<1-6>|preference]

accounting server preference [auth-server-host|auth-server-number|none]

accounting server <1-6> [dscp|host|nai-routing|onboard|proxy-mode|retry-timeout-
factor|timeout]

accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]

accounting server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2
<SECRET>|<SECRET>] {port <1-65535>}

accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT>
{strip}

accounting server <1-6> onboard [centralized-controller|self|controller]

accounting server <1-6> proxy-mode [none|through-centralized-controller|through-
controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]

accounting server <1-6> timeout <1-60> {attempts <1-10>}

accounting type [start-interim-stop|start-stop|stop-only]
```

Parameters

- `accounting interim interval <60-3600>`

interim	Configures the interim accounting interval. This is the interval at which interim accounting updates are posted to the accounting server.
interval <60-3000>	Specify the interim interval from 60 - 3600 seconds. The default is 1800 seconds.

- `accounting server preference [auth-server-host|auth-server-number|none]`

server	Configures a RADIUS accounting server's settings
preference	Configures the accounting server's preference mode. Authentication requests are forwarded to a accounting server, from the pool, based on the preference mode selected.
auth-server-host	Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is identified by its hostname.

auth-server-number	Sets the authentication server as the accounting server This parameter indicates the same server is used for authentication and accounting. The server is identified by its index or number.
none	Indicates the accounting server is independent of the authentication server

- `accounting server <1-6> [dscp <0-63>|retry-timeout-factor <50-200>]`

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
dscp <0-63>	Sets the *Differentiated Services Code Point* (DSCP) value for *Quality of Service* (QOS) monitoring. This value is used in generated RADIUS packets. • <0-63> – Sets the DSCP value from 0 - 63. The default value is 34.
retry-timeout-factor <50-200>	Sets the scaling factor for retransmission timeouts. The timeout at each attempt is a function of this retry-timeout factor and the attempt number. • <50-200> – Specify a value from 50 - 200. The default is 100. If the scaling factor is 100, the interval between two consecutive retries remains the same, irrespective of the number of retries. If the scaling factor is less than 100, the interval between two consecutive retires reduces with subsequent retries. If this scaling factor is greater than 100, the interval between two consecutive retries increases with subsequent retries.

- `accounting server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>] {port <1-65535>}`

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
host <IP/ HOSTNAME/HOST-ALIAS>	Configures the accounting server's hostname IP address, or host-alias The host alias should be existing and configured.
secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Configures a common secret key used to authenticate with the accounting server • 0 <SECRET> – Configures a clear text secret key • 2 <SECRET> – Configures an encrypted secret key • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters.
port <1-65535>	Optional. Configures the accounting server's UDP port (the port used to connect to the accounting server) • <1-65535> – Sets the port number from 1 - 65535 (default port is 1813)

- `accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-TEXT> {strip}`

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.

nai-routing	Enables *Network Access Identifier* (NAI) routing. This option is disabled by default. The NAI is a character string in the format of an e-mail address as either *user* or *user@realm* but it need not be a valid e-mail address or a fully qualified domain name. AAA servers identify clients using the NAI. The NAI can be used either in a *specific* or *generic* form. The specific form, which must contain the user portion and may contain the @realm portion, identifies a single user. Using the generic form allows all users to be configured on a single command line, irrespective of whether the users are within a realm or not. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dial up ISPs. With NAI, an ISP does not have the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers as need be.
realm-type	Specifies whether the prefix or suffix of the username is used as the match criteria. For example, if the option selected is prefix, the username's prefix is matched to the realm.
[prefix|suffix]	Select one of the following options: • prefix – Matches the prefix of the username (For example, username is of type DOMAIN/user1, DOMAIN/user2). This is the default setting. • suffix – Matches the suffix of the username (For example, user1@DOMAIN, user2)@DOMAIN)
realm <REALM-TEXT>	Configures the text matched against the username. Enter the realm name (should not exceed 50 characters). When the RADIUS accounting server receives a request for a user name, the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server. • <REALM-TEXT> – Specifies the matching text including the delimiter (a delimiter is typically '' or '@')
strip	Optional. When enabled, strips the realm from the username before forwarding the request to the RADIUS server. This option is disabled by default.

- `accounting server <1-6> onboard [centralized-controller|self|controller]`

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
onboard	Selects an onboard server instead of an external host
centralized-controller	Configures the server on the centralized controller managing the network
self	Configures the onboard server on a AP, wireless controller, or service platform (where the client is associated)
controller	Configures local RADIUS server settings

- `accounting server <1-6> proxy-mode [none|through-centralized-controller|through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]`

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
proxy-mode	Select the mode used to proxy requests. The options are: none, through-controller, and through-rf-domain-manager.
none	No proxy required. Sends the request directly using the IP address of the device. This is the default setting.
through-centralized-controller	Proxy requests through the centralized controller that is configuring and managing the network

through-controller	Proxies requests through the controller (access point, wireless controller, or service platform) configuring the device
through-mint-host <HOSTNAME/MINT-ID>	Proxies requests through a neighboring MiNT device. Provide the device's MiNT ID or hostname.
through-rf-domain-manager	Proxies requests through the local RF Domain Manager

- `accounting server <1-6> timeout <1-60> {attempts <1-10>}`

server <1-6>	Configures an accounting server. Up to 6 accounting servers can be configured.
timeout <1-60>	Configures the timeout for each request sent to the RADIUS server • <1-60> – Specify a value from 1 - 60 seconds. The default is 5 seconds.
attempts <1-10>	Optional. Specifies the number of times a transmission request is attempted • <1-10> – Specify a value from 1 - 10. The default is 3.

- `accounting type [start-interim-stop|start-stop|stop-only]`

type	Configures the type of RADIUS accounting packets sent. The options are: start-interim-stop, start-stop, and stop-only.
start-interim-stop	Sends accounting-start and accounting-stop messages when the session starts and stops. This parameter also sends interim accounting updates.
start-stop	Sends accounting-start and accounting-stop messages when the session starts and stops. This is the default setting.
stop-only	Sends an accounting-stop message when the session ends

Example

```
rfs6000-37FABE(config-aaa-policy-test)#accounting interim interval 65

rfs6000-37FABE(config-aaa-policy-test)#accounting server 2 host 172.16.10.10
secret test1 port 1
rfs6000-37FABE(config-aaa-policy-test)#accounting server 2 timeout 2 attempts 2
rfs6000-37FABE(config-aaa-policy-test)#accounting type start-stop
rfs6000-37FABE(config-aaa-policy-test)#accounting server preference auth-server-
number

rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 accounting interim interval 65
 accounting server preference auth-server-number
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Removes or resets accounting server parameters

8.1.2 attribute

aaa-policy

Configures RADIUS Framed-MTU attribute used in access and accounting requests. The Framed-MTU attribute reduces the *Extensible Authentication Protocol* (EAP) packet size of the RADIUS server. This command is useful in networks where routers and firewalls do not perform fragmentation.

To ensure network security, some firewall software drop UDP fragments from RADIUS server EAP packets. Consequently, the packets are large. Using Framed MTU reduces the packet size. EAP authentication uses Framed MTU to notify the RADIUS server about the *Maximum Transmission Unit* (MTU) negotiation with the client. The RADIUS server communications with the client do not include EAP messages that cannot be delivered over the network.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622,, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-
vsa|framed-ip-address|framed-mtu|location-information|nas-ip-address|nas-ipv6-
address|operator-name|service-type]

attribute acct-delay-time
attribute acct-multi-session-id
attribute chargeable-user-identity
attribute cisco-vsa audit-session-id
attribute framed-ip-address
attribute framed-mtu <100-1500>
attribute location-information [include-always|none|server-requested]
attribute nas-ip-address <WORD>
attribute nas-ipv6-address
attribute operator-name <OPERATOR-NAME>
attribute service-type [framed|login]
```

Parameters

- `attribute acct-delay-time`

acct-delay-time	Enables support for *accounting-delay-time* attribute in accounting requests. When enabled, this attribute indicates the number of seconds the client has been trying to send a request to the accounting server. By subtracting this value from the time the packet is received by the server, the system is able to calculate the time of a request-generating event. Note, the network transit time is ignored. This option is disabled by default. Including the *acct-delay-time* attribute in accounting requests updates the acct-delay-time value whenever the packet is retransmitted, This changes the content of the attributes field, requiring a new identifier and request authenticator.

- `attribute acct-multi-session-id`

acct-multi-session-id	Enables support for *accounting-multi-session-id* attribute. When enabled, it allows linking of multiple related sessions of a roaming client. This option is useful in scenarios where a client roaming between access points sends multiple RADIUS accounting requests to different access points. This option is disabled by default.

- `attribute chargeable-user-identity`

chargeable-user-identity	Enables support for chargeable-user-identity attribute. This option is disabled by default.

- `attribute cisco-vsa audit-session-id`

cisco-vsa audit-session-id	Configures the CISCO *Vendor Specific Attribute* (VSA) attribute included in access requests. This feature s disabled by default. This VSA allows CISCO's *Identity Services Engine* (ISE) to validate a requesting client's network compliance, such as the validity of virus definition files (anti virus software or definition files for an anti-spyware software application). • audit-session-id – Includes the audit session ID attribute in access requests The audit session ID is included in access requests when Cisco ISE is configured as an authentication server. **Note:** If the Cisco VSA attribute is enabled, configure an additional UDP port to listen for dynamic authorization messages from the Cisco ISE server. For more information, see *service*.

- `attribute framed-ip-address`

framed-ip-address	Enables inclusion of framed IP address attribute in access requests. This option is disabled by default.

- `attribute framed-mtu <100-1500>`

framed-mtu <100-1500>	Configures Framed-MTU attribute used in access requests • <100-1500> – Specify the Framed-MTU attribute from 100 - 1500. The default value is 1400.

- `attribute location-information [include-always|none|server-requested]`

location-information [include-always| none|server-requested]	Enables support for RFC5580 location information attribute, based on the option selected. The various options are: • include-always – Always includes location information in RADIUS authentication and accounting messages • none – Disables sending of location information in RADIUS authentication and accounting messages. This is the default setting. • server-requested – Includes location information in RADIUS authentication and accounting messages only when requested by the server When enabled, location information is exchanged in authentication and accounting messages.

- `attribute nas-ip-address <WORD>`

nas-ip-address <WORD>	Enables configuration of an IP address, which is used as the RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. If you are using a cluster of small network access servers (NASs) to simulate a large NAS, use this option to improve scalability. The IP address configured using this option allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server. • <WORD> – Provide the IPv4 address.

- `attribute nas-ipv6-address`

nas-ipv6-address	Enables support for NAS IPv6 address. This option is disabled by default. When enabled, IPv6 addresses are assigned to hosts. The length of IPv4 and IPv6 addresses is 32-bit and 128-bit respectively. Consequently, an IPv6 address requires a larger address space.

- `attribute operator-name <OPERATOR-NAME>`

operator-name <OPERATOR-NAME>	Enables support for RFC5580 operator name attribute. When enabled, the network operator's name is included in all RADIUS authentication and accounting messages and uniquely identifies the access network owner. This option is disabled by default. • <OPERATOR-NAME> – Specify the network operator's name (should not exceed 63 characters in length).

- `attribute service-type [framed|login]`

service-type [framed|login]	Configures the service-type (6) attribute value. This attribute identifies the following: the type of service requested and the type of service to be provided. • framed – Sets service-type to *framed (2)* in the authentication packets. When enabled, a framed protocol, *Point-to-Point Protocol* (PPP) or *Serial Line Internet Protocol* (SLIP), is started for the client. This is the default setting. • login – Sets service-type to *login (1)* in the authentication packets. When enabled, the client is connected to the host.

Example

```
rfs6000-37FABE(config-aaa-policy-test)#attribute framed-mtu 110
rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 accounting interim interval 65
 accounting server preference auth-server-number
 attribute framed-mtu 110
rfs6000-37FABE(config-aaa-policy-test)#

rfs6000-37FABE(config-aaa-policy-test1)#attribute cisco-vsa audit-session-id

rfs6000-37FABE(config-aaa-policy-test1)#show context
aaa-policy test
 attribute cisco-vsa audit-session-id
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Resets values or disables commands

8.1.3 authentication

aaa-policy

Configures user authentication parameters

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
authentication [eap|protocol|server]

authentication eap wireless-client [attempts <1-10>|identity-request-retry-
timeout <10-5000>|identity-request-timeout <1-60>|retry-timeout-factor <50-200>|
timeout <1-60>]

authentication protocol [chap|mschap|mschapv2|pap]

authentication server <1-6> [dscp|host|nac|nai-routing|onboard|proxy-mode|retry-
timeout-factor|timeout]

authentication server <1-6> dscp <0-63>

authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2
<SECRET>|<SECRET>] {port <1-65535>}

authentication server <1-6> nac

authentication server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-
NAME>{strip}

authentication server <1-6> onboard [centralized-controller|controller|self]

authentication server <1-6> proxy-mode [none|through-centralized-controller|
through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-
manager]

authentication server <1-6> retry-timeout-factor <50-200>

authentication server <1-6> timeout <1-60> {attempts <1-10>}
```

Parameters

```
• authentication eap wireless-client [attempts <1-10>|identity-request-retry-
timeout <10-5000>|identity-request-timeout <1-60>|retry-timeout-factor <50-
200>|timeout <1-60>]
```

eap	Configures EAP authentication parameters
wireless-client	Configures wireless client's EAP parameters
attempts <1-10>	Configures the maximum number of attempts allowed to authenticate a wireless client • <1-10> – Specify a value from 1 - 10. The default is 3.
identity-request-retry-timeout <10-5000>	Configures the interval, in milliseconds, after which an EAP-identity request to the wireless client is retried • <10-5000> – Specify a value from 10 - 5000 milliseconds. The default is 1000 milliseconds.

identity-request-timeout <1-60>	Configures the timeout, in seconds, after the last EAP-identity request message retry attempt (to allow time to manually enter user credentials) • <1-60> – Specify a value from 1 - 60 seconds. The default is 30 seconds.
retry-timeout-factor <50-200>	Configures the spacing between successive EAP retries • <50-200> – Specify a value from 50 - 200. The default is 100. A value of 100 indicates the interval between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.
timeout <1-60>	Configures the interval, in seconds, between successive EAP-identity request sent to a wireless client • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.

- `authentication protocol [chap|mschap|mschapv2|pap]`

protocol [chap|mschap|mschapv2|pap]	Configures one of the following protocols for non-EAP authentication: • chap – Uses *Challenge Handshake Authentication Protocol* (CHAP) • mschap – Uses *Microsoft Challenge Handshake Authentication Protocol* (MS-CHAP) • mschapv2 – Uses MS-CHAP version 2 • pap – Uses *Password Authentication Protocol* (PAP) (default authentication protocol used)

- `authentication server <1-6> dscp <0-63>`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
dscp <0-63>	Configures the *Differentiated Service Code Point* (DSCP) quality of service parameter generated in RADIUS packets. The DSCP value specifies the class of service provided to a packet, and is represented by a 6-bit parameter in the header of every IP packet. • <0-63> – Specify the value from 0 - 63. The default is 46.

- `authentication server <1-6> host <IP/HOSTNAME/HOST-ALIAS> secret [0 <SECRET>|2 <SECRET>|<SECRET>] {port <1-65535>}`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
host <IP/HOSTNAME/HOST-ALIAS>	Sets the RADIUS authentication server's IP address, hostname, or host-alias The host alias should be existing and configured.

secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Configures the RADIUS authentication server's secret. This key is used to authenticate with the RADIUS server. • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters in length.
port <1-65535>	Optional. Specifies the RADIUS authentication server's UDP port (this port is used to connect to the RADIUS server) • <1-65535> – Specify a value from 1 - 65535. The default port is 1812.

- `authentication server <1-6> nac`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
nac	Enables *Network Access Control* (NAC) on the RADIUS authentication server identified by the <1-6> parameter. Using NAC, the controller hardware and software grant access to specific network resources. NAC performs a user and client authorization check for resources that do not have a NAC agent. NAC verifies the client's compliance with the controller's security policy. The controller supports only the EAP/802.1x type of NAC. However, the controller also provides a means to bypass NAC authentication for client's that do not have NAC 802.1x support (printers, phones, PDAs, etc.).

- `accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <REALM-NAME> {strip}`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specifies the RADIUS server index from 1 - 6.
nai-routing	Enables NAI routing. When enabled, AAA servers identify clients using NAI. This option is disabled by default. The NAI is a character string in the format of an e-mail address as either *user* or *user@realm* but it need not be a valid e-mail address or a fully qualified domain name. AAA servers identify clients using the NAI. The NAI can be used either in a *specific* or *generic* form. The specific form, which must contain the user portion and may contain the @realm portion, identifies a single user. Using the generic form allows all users to be configured on a single command line, irrespective of whether the users are within a realm or not. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dial up ISPs. With NAI, an ISP does not have the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers as need be.
realm-type [prefix|suffix]	Configures the realm-type used for NAI authentication • prefix – Sets the realm prefix. For example, in the realm name 'AC\JohnTalbot', the prefix is 'AC' and the user name 'JohnTalbot'. • suffix – Sets the realm suffix. For example, in the realm name 'JohnTalbot@AC.org' the suffix is 'AC.org' and the user name is 'JohnTalbot'.

realm <REALM-NAME>	Sets the realm information used for RADIUS authentication. The realm name should not exceed 64 characters in length. When the wireless controller or access point's RADIUS server receives a request for a user name the server references a table of usernames. If the user name is known, the server proxies the request to the RADIUS server. • <REALM-NAME> – Sets the realm used for authentication. This value is matched against the user name provided for RADIUS authentication. Example: Prefix - AC\JohnTalbot Suffix - JohnTalbot@AC.org
strip	Optional. Indicates the realm name must be stripped from the user name before sending it to the RADIUS server for authentication. For example, if the complete username is 'AC\JohnTalbot', then with the *strip* parameter enabled, only the 'JohnTalbot' part of the complete username is sent for authentication. This option is disabled by default.

- `authentication server <1-6> onboard [centralized-controller|controller|self]`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
onboard [centralized-controller| controller|self]	Selects the onboard RADIUS server for authentication instead of an external host • centralized-controller – Configures the server on the centralized controller managing the network • controller – Configures the wireless controller, to which the AP is adopted, as the onboard wireless controller • self – Configures the onboard server on the device (AP or wireless controller) where the client is associated as the onboard wireless controller

- `authentication server <1-6> proxy-mode [none|through-centralized-controller|through-controller|through-mint-host <HOSTNAME/MINT-ID>|through-rf-domain-manager]`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
proxy-mode [none| through-centralized-controller| through-controller| through-mint-host <HOSTNAME/MINT-ID>| through-rf-domain-manager]	Configures the mode for proxying a request • none – Proxying is not done. The packets are sent directly using the IP address of the device. This is the default setting. • through-centralized-controller – The traffic is proxied through the centralized controller that is configuring and managing the network. • through-controller – The traffic is proxied through the wireless controller configuring this device. • through-mint-host <HOSTNAME/MINT-ID> – The traffic is proxied through a neighboring MiNT device. Provide the device's hostname or MiNT ID. • through-rf-domain-manager – The traffic is proxied through the local RF Domain manager.

- `authentication server <1-6> retry-timeout-factor <50-200>`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
retry-timeout-factor <50-200>	Configures the scaling of timeouts between two consecutive RADIUS authentication retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between two consecutive retries increases with each successive retry.

- `authentication server <1-6> timeout <1-60> {attempts <1-10>}`

server <1-6>	Configures a RADIUS authentication server. Up to 6 RADIUS servers can be configured. • <1-6> – Specify the RADIUS server index from 1 - 6.
timeout <1-60>	Configures the timeout, in seconds, for each request sent to the RADIUS server. This is the time allowed to elapse before another request is sent to the RADIUS server. If a response is received from the RADIUS server within this time, no retry is attempted. • <1-60> – Specify a value from 1 - 60 seconds. The default is 3 seconds.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10. The default is 3.

Example

```
rfs6000-37FABE(config-aaa-policy-test)#authentication server 5 host 172.16.10.10
secret 0 test1 port 1

rfs6000-37FABE(config-aaa-policy-test)#authentication server 5 timeout 10 attempts
3

rfs6000-37FABE(config-aaa-policy-test)#authentication protocol chap

rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 attribute framed-mtu 110
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Resets authentication parameters on this AAA policy

8.1.4 health-check

aaa-policy

An AAA server could go offline. When a server goes offline, it is marked as *down*. This command configures the interval after which a server marked as *down* is checked to see if it has come back online and is reachable.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
health-check interval <60-86400>
```

Parameters

- `health-check interval <60-86400>`

interval <60-86400>	Configures an interval (in seconds) after which a down server is checked to see if it is reachable again • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 3600 seconds.

Example

```
rfs6000-37FABE(config-aaa-policy-test)#health-check interval 4000

rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 health-check interval 4000
 attribute framed-mtu 110
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Resets the health-check interval for AAA servers

8.1.5 mac-address-format

aaa-policy

Configures the format MAC addresses are filled in RADIUS request frames

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot] case
[lower|upper] attributes [all|username-password]
```

Parameters]

```
• mac-address-format [middle-hyphen|no-delim|pair-colon|pair-hyphen|quad-dot]
case [lower|upper] attributes [all|username-password]
```

middle-hyphen	Configures the MAC address format as AABBCC-DDEEFF
no-delim	Configures the MAC address format as AABBCCDDEEFF (without delimiters)
pair-colon	Configures the MAC address format as AA:BB:CC:DD:EE:FF
pair-hyphen	Configures the MAC address display format as AA-BB-CC-DD-EE-FF (default setting)
quad-dot	Configures the MAC address display format as AABB.CCDD.EEFF
case [lower|upper]	Indicates the case the MAC address is formatted • lower – Indicates MAC address is in lower case. For example, aa:bb:cc:dd:ee:ff • upper – Indicates MAC address is in upper case. For example, AA:BB:CC:DD:EE:FF (default setting)
attributes [all|username-password]	Configures RADIUS attributes to which this MAC format is applicable • all – Applies to all attributes with MAC addresses such as username, password, calling-station-id, and called-station-id • username-password – Applies only to the username and password fields (default setting)

Example

```
rfs6000-37FABE(config-aaa-policy-test)#mac-address-format quad-dot case upper
attributes username-password

rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 mac-address-format quad-dot case upper attributes username-password
 authentication protocol chap
 --More--
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Resets the MAC address format to default (pair-hyphen)

8.1.6 no

aaa-policy

Negates a AAA policy command or sets its default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [accounting|attribute|authentication|health-check|mac-address-format|proxy-attribute|server-pooling-mode|use]

no accounting interim interval

no accounting server preference

no accounting server <1-6> {dscp|nai-routing|proxy-mode|retry-timeout-factor|timeout}

no accounting type

no attribute [acct-delay-time|acct-multi-session-id|chargeable-user-identity|cisco-vsa audit-session-id|framed-ip-address|framed-mtu|location-information|nas-ipv6-address|operator-name|service-type]

no authentication [eap|protocol|server]

no authentication eap wireless-client [attempts|identity-request-retry-timeout|identity-request-timeout|retry-timeout-factor|timeout]

no authentication protocol

no authentication server <1-6> {dscp|nac|nai-routing|proxy-mode|retry-timeout-factor|timeout}

no health-check interval

no mac-address-format

no proxy-attribute [nas-identifier|nas-ip-address]

no server-pooling-mode

no use nac-list
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates a AAA policy command or sets its default

Example

The following example shows the AAA policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 accounting server 2 timeout 2 attempts 2
 mac-address-format quad-dot case upper attributes username-password
 authentication protocol chap
 accounting interim interval 65
 accounting server preference auth-server-number
 health-check interval 4000
 attribute framed-mtu 110
rfs6000-37FABE(config-aaa-policy-test)#

rfs6000-37FABE(config-aaa-policy-test)#no accounting server 2 timeout 2
rfs6000-37FABE(config-aaa-policy-test)#no accounting interim interval
rfs6000-37FABE(config-aaa-policy-test)#no health-check interval
rfs6000-37FABE(config-aaa-policy-test)#no attribute framed-mtu
rfs6000-37FABE(config-aaa-policy-test)#no authentication protocol
```

The following example shows the AAA policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
rfs6000-37FABE(config-aaa-policy-test)#
```

8.1.7 proxy-attribute

aaa-policy

Configures RADIUS server's attribute behavior when proxying through a wireless controller or a RF Domain manager

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
proxy-attribute [nas-identifier|nas-ip-address]
proxy-attribute [nas-identifier [originator|proxier]|nas-ip-address
[none|proxier]]
```

Parameters

```
• proxy-attribute [nas-identifier [originator|proxier]|nas-ip-address
[none|proxier]]
```

nas-identifier [originator|proxier]	Uses NAS identifier • originator – Configures the NAS identifier as the originator of the RADIUS request. The originator could be an AP, or a wireless controller with radio. This is the default setting. • proxier – Configures the proxying device as the NAS identifier. The device could be a controller or a RF Domain manager.
nas-ip-address [none|proxier]	Uses NAS IP address • none – NAS IP address attribute is not filled • proxier – NAS IP address is filled by the proxying device.The device could be a controller or a RF Domain manager. This is the default setting.

Example

```
rfs6000-37FABE(config-aaa-policy-test)#proxy-attribute nas-ip-address proxier

rfs6000-37FABE(config-aaa-policy-test)#proxy-attribute nas-identifier originator
```

Related Commands

no	Resets RADIUS server's proxying attributes

8.1.8 server-pooling-mode

Configures the server selection method from a pool of AAA servers. The available methods are *failover* and *load-balance*.

In the failover scenario, when a configured AAA server goes down, the server with the next higher index takes over for the failed server.

In the load-balance scenario, when a configured AAA server goes down, the remaining servers distribute the load amongst themselves.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
server-pooling-mode [failover|load-balance]
```

Parameters

- `server-pooling-mode [failover|load-balance]`

failover	Sets the pooling mode to failover. This is the default setting. When a configured AAA server fails, the server with the next higher index takes over the failed server's load.
load-balance	Sets the pooling mode to load balancing When a configured AAA server fails, all servers in the pool share the failed server's load transmitting requests in a round-robin fashion.

Example

```
rfs6000-37FABE(config-aaa-policy-test)#server-pooling-mode load-balance

rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test2 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 server-pooling-mode load-balance
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Resets the method of selecting a server, from the pool of configured AAA servers

8.1.9 use

aaa-policy

Associates a *Network Access Control* (NAC) with this AAA policy. This allows only the set of configured devices to use the configured AAA servers.

For more information on creating a NAC list, see *nac-list*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use nac-list <NAC-LIST-NAME>
```

Parameters

- `use nac-list <NAC-LIST-NAME>`

nac-list <NAC-LIST-NAME>	Associates a NAC list with this AAA policy • <NAC-LIST-NAME> – Specify the NAC list name (should be existing and configured).

Example

```
rfs6000-37FABE(config-aaa-policy-test)#use nac-list test1

rfs6000-37FABE(config-aaa-policy-test)#show context
aaa-policy test
 authentication server 5 host 172.16.10.10 secret 0 test1 port 1
 authentication server 5 timeout 10
 accounting server 2 host 172.16.10.10 secret 0 test1 port 1
 server-pooling-mode load-balance
 mac-address-format quad-dot case upper attributes username-password
 accounting server preference auth-server-number
 health-check interval 4000
use nac-list test1
rfs6000-37FABE(config-aaa-policy-test)#
```

Related Commands

no	Resets set values or disables commands
nac-list	Creates a NAC list

9 AUTO-PROVISIONING-POLICY

This chapter summarizes the auto provisioning policy commands in the CLI command structure.

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt multiple access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device uses auto provisioning policies to determine which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Auto provisioning or adoption is the process by which an access point discovers controllers in the network, identifies the most desirable controller, associates with the identified controller, and optionally obtains an image upgrade, obtains its configuration and considers itself provisioned.

At adoption, an access point solicits and receives multiple adoption responses from controllers available on the network. These adoption responses contain loading policy information the access point uses to select the optimum controller for adoption. An auto-provisioning policy maps a new AP to a profile and RF Domain based on various parameters related to the AP and where it is connected. By default a new AP will be mapped to the default profile and default RF Domain. Modify existing auto-provisioning policies or create a new one as needed to meet the configuration requirements of a device.

An auto-provisioning policy enables an administrator to define rules for the supported access points capable of being adopted by a controller. The policy determines which configuration policies are applied to an adoptee based on its properties. For example, a configuration policy could be assigned based on MAC address, IP address, *CISCO Discovery Protocol* (CDP) snoop strings, etc. Once created an auto provisioning policy can be used in profiles or device configuration objects. The policy contains a set of rules (ordered by precedence) that either deny or allow adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

For example,

```
rule #1 adopt ap7161 10 profile default vlan 10
rule #2 adopt ap6562 20 profile default vlan 20
rule #3 adopt ap7161 30 profile default serial-number
rule #4 adopt ap7161 40 p d mac aa bb
```

AP7161 L2 adoption, VLAN 10 - will use rule #1

AP7161 L2 adoption, VLAN 20 - will not use rule #2 (wrong type), may use rule #3 if the serial number matched, or rule #4

If aa<= MAC <= bb, or else default.

With the implementation of the *hierarchically managed* (HM) network, the auto-provisioning policy has been modified to enable controllers to adopt other controllers in addition to access points.

The new WiNG HM network defines a three-tier structure, consisting of multiple wireless sites managed by a single *Network Operations Center* (NOC) controller, The NOC controller constitutes the first and the site controllers constitute the second tier of the hierarchy. The site controllers in turn adopt and manage access points that form the third tier of the hierarchy.

All adopted devices (access points and second-level controllers) are referred to as the ‘adoptee’. The adopting devices are the ‘adopters’.

A controller cannot be configured as an adoptee and an adopter simultaneously. In other words, a controller can either be an adopter (adopts another controller) or an adoptee (is adopted by another controller). Therefore, a site controller, which has been adopted by a NOC controller, cannot adopt another controller.

A controller should be configured to specify the device types (APs and/or controllers) that it can adopt. For more information on configuring the adopted-device types for a controller, see *controller*.

NOTE: The adoption capabilities of a controller depends on:

- Whether the controller is deployed at the NOC or site
  - A NOC controller can adopt site controllers and access points
  - A site controller can only adopt access points
- The controller device type, which determines the number and type of devices it can adopt

NOTE: Some access points can be configured as virtual controllers. When configured as a virtual controller, an AP can only adopt another AP of the same type. In such a scenario, an auto provisioning policy is required to enable adoption of a specific device identified by its MAC address, IP address, serial number, model number, etc.

Use the (config) instance to configure an auto-provisioning policy. To navigate to the auto-provisioning-policy configuration instance, use the following command:

```
<DEVICE>(config)#auto-provisioning-policy <POLICY-NAME>

nx9500-6C8809((config)#auto-provisioning-policy test
nx9500-6C8809((config-auto-provisioning-policy-test)#?
Auto-Provisioning Policy Mode commands:
  adopt                       Add rule for device adoption
  auto-create-rfd-template    When RF Domain specified by the matching rule
                              template does not exist create new RF Domain
                              automatically
  default-adoption            Adopt devices even when no matching rules are
                              found. Assign default profile and default
                              rf-domain
  deny                        Add rule to deny device adoption
  evaluate-always             Set the flag to evaluate the policy everytime,
                              regardless of previous adoption status
  no                          Negate a command or set its defaults
  redirect                    Add rule to redirect device adoption
  upgrade                     Add rule for device upgrade

  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or terminal
nx9500-6C8809((config-auto-provisioning-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

9.1 auto-provisioning-policy

- *AUTO-PROVISIONING-POLICY*

The following table summarizes auto provisioning policy configuration commands:

Table 9.1 *Auto-Provisioning-Policy-Config Commands*

Command	Description	Reference
adopt	Adds a permit adoption rule	*page 9-5*
auto-create-rfd-template	Enables auto creation of a new RF Domain based on an existing RF Domain template specified using this command	*page 9-10*
default-adoption	Adopts devices even when no matching rules are found. Assigns default profile and default RF Domain	*page 9-12*
deny	Adds a deny adoption rule	*page 9-13*
evaluate-always	Runs this policy every time a device is adopted	*page 9-16*
redirect	Adds a rule redirecting device adoption to a specified controller within the system	*page 9-17*
upgrade	Adds a device upgrade rue to this auto provisioning policy	*page 9-21*
no	Negates a command or reverts settings to their default	*page 9-24*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

9.1.1 adopt

auto-provisioning-policy

Adds device adoption rules

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
adopt [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]

adopt [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[profile|rf-domain]

adopt [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7632|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] [any|area|cdp-match|
dhcp-option|floor|fqdn|ip|ipv6|lldp-match|mac|model-number|rf-domain|
serial-number|vlan]

adopt [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any

adopt [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] [area <AREA-NAME>|
cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|floor <FLOOR-NAME>|fqdn
<FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]
|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-
NUMBER>|serial-number <SERIAL-NUMBER>|rf-domain <RF-DOMAIN-NAME>|vlan <VLAN-ID>]
```

Parameters

```
• adopt [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] any
```

adopt	Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX7500, NX7510, NX7520, NX7530 NX95XX, VX9000, and NX9600. Note: 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type.

precedence <1-10000>	Sets the rule precedence from 1 - 10000. A rule with a lower value has a higher precedence.
profile <DEVICE-PROFILE-NAME>	Sets the device profile for this provisioning policy. The selected device profile must be appropriate for the device being provisioned. For example, use an AP7502 device profile for an AP7502. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name. Provide a device profile name (should be existing and configured). Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor'. Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system.
rf-domain <RF-DOMAIN-NAME>	Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name OR use a string alias to identify the RF Domain. Provide the full RF Domain name or an alias (should be existing and configured). Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]' Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system. **Note:** Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.example_company.com'. In this example, the string-alias *$DOMAIN* is mapped to the string: *test.example_company.com*. For more information, see *alias*.
any	Indicates any device. Any device seeking adoption is adopted.

- `adopt[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|nx9000|vx9000|nx9600] precedence <1-10000> [profile <DEVICE-PROFILE-NAME>|rf-domain <RF-DOMAIN-NAME>] [area <AREA-NAME>|cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|floor <FLOOR-NAME>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-NUMBER>|rf-domain <RF-DOMAIN-NAME>|vlan <VLAN-ID>]`

adopt	Adds an adopt device rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7502, AP7522, AP7532, AP7562, AP7161, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX7500, NX7510, NX7520, NX7530, NX95XX, VX9000, and NX9600. **Note:** 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type.
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence.

profile <DEVICE-PROFILE-NAME>	Sets the device profile for this provisioning policy. The selected device profile must be AP7502 for the device being provisioned. For example, use an AP7502 device profile for an AP7502. Using an inappropriate device profile can result in unpredictable results. Provide a device profile name (should be existing and configured). Or a template with appropriate substitution tokens, such as 'campus-$MODEL[1:6]', 'FQDN[1:4]-indoor' Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system.
rf-domain <RF-DOMAIN-NAME>	Sets the RF Domain for this auto provisioning policy. The provisioning policy is only applicable to devices that try to become a part of the specified RF Domain. Provide the full RF Domain name or an alias (should be existing and configured). Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]'. Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system. **Note:** Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.example_company.com'. In this example, the string-alias *$DOMAIN* is mapped to the string: *test.example_company.com*. For more information, see *alias*.
area <AREA-NAME>	Matches the area of deployment. This option is not applicable to the 'rf-domain' parameter. • <AREA-NAME> – Enter a 64 character maximum deployment area name assigned to this policy. Devices with matching area names are adopted.
cdp-match <LOCATION-SUBSTRING>	Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com, 'controller1', 'example', 'example.com', are examples of the substrings that will match. • <LOCATION-SUBSTRING> – Specify the value to match. Devices matching the specified value are adopted.
dhcp-option <DHCP-OPTION>	Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present. • <DHCP-OPTION> – Specify the DHCP option. Devices matching the specified value are adopted.
floor <FLOOR-NAME>	Matches the floor name. This option is not applicable to the 'rf-domain' parameter. • <FLOOR-NAME> – Enter a 32 character maximum deployment floor name assigned to this policy. Devices with matching floor names are adopted.
fqdn <FQDN>	Matches a substring to the *Fully Qualified Domain Name* (FQDN) of a device (case insensitive) FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. This parameter allows a device to adopt based on its FQDN value. • <FQDN> – Specify the FQDN. Devices matching the specified value are adopted.

ip [<START-IP> <END-IP>| <IP/MASK>]	Adopts a device if its IP address matches the specified IPv4 address or is within the specified IP address range. Or if the device is a part of the specified subnet. • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Adopts a device if its IP v6 address matches the specified IPv6 address or is within the specified IP address range. Or if the device is a part of the specified subnet. • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IPv6 address.
lldp-match <LLDP-STRING>	Matches a substring in a list of *Link Layer Discovery Protocol* (LLDP) snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com, and controller3.example.com,'controller1', 'example', 'example.com', are examples of the substrings that will match. LLDP is a vendor neutral link layer protocol that advertises a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the LLDP string. Devices matching the specified value are adopted.
mac <START-MAC> {<END-MAC>}	Adopts a device if its MAC address matches the specified MAC address or is within the specified MAC address range • <START-MAC> – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Adopts a device if its model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number.
rf-domain <RF-DOMAIN-NAME>	Adopts a device if its RF Domain matches <RF-DOMAIN-NAME> <RF-DOMAIN-NAME> – Specify the RF Domain name. You can use a string alias to specify a RF Domain. Provide the full RF Domain name or an alias (should be existing and configured). Or a template with appropriate substitution tokens, such as '$CDP[1:7]', '$DNS-SUFFIX[1:5]' Please see the Usage Guidelines section *Built-in Tokens & Alias* for the different types of built in tokens available in the system. **Note:** Use the built-in string alias or a user-defined string alias. String aliases allow you to configure APs in the same RF Domain as the adopting controller. A string alias maps a name to an arbitrary string value, for example, 'alias string $DOMAIN test.example_company.com'. In this example, the string-alias *$DOMAIN* is mapped to the string: *test.example_company.com*. For more information, see *alias*.
serial-number <SERIAL-NUMBER>	Adopts a device if its serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number.
vlan <VLAN-ID>	Adopts a device if its VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID.

Usage Guidelines Built-in Tokens & Alias

Following are the built-in tokens that can be used to identify the devices to adopt:

```
$FQDN        - references FQDN of adopting device
$CDP         - references CDP Device Id of the wired switch to which
               adopting device is connected
$LLDP        - references LLDP System Name of wired switch to
               which adopting device is connected
$DHCP        - references DHCP Option Value received by the
               adopting device
$SN          - references SERIAL NUMBER of adopting device
$MODEL       - references MODEL NUMBER of adopting device
$DNS-SUFFIX - references FQDN excluding the hostname of the
               adopting device
$CDP-SUFFIX - references CDP excluding the hostname of the
               adopting device
$LLDP-SUFFIX - references LLDP excluding the hostname of the
               adopting device
```

Following is the built-in alias that can be used to identify the RF Domain of devices to adopt:

```
$AUTO-RF-DOMAIN - rf-domain of adopting device
```

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#adopt ap81xx precedence 1
profile default-ap81xx vlan 1

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap81xx precedence 1 profile default-ap81xx vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#show wireless ap configured
-------------------------------------------------------------------------------
-------
 IDX      NAME              MAC             PROFILE       RF-DOMAIN       ADOPTED-BY
-------------------------------------------------------------------------------
-------
 1   ap81xx-711728    B4-C7-99-71-17-28   default-ap81xx   default    00-23-68-22-
9D-58
 2   rfs4000-229D58   00-23-68-22-9D-58   default-rfs4000  default
-------------------------------------------------------------------------------
-------
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs6000-6DCD4B(config-auto-provisioning-policy-test)#adopt anyap precedence 1
profile rfs6000 any

rfs6000-6DCD4B(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt anyap precedence 1 profile rfs6000 any
rfs6000-6DCD4B(config-auto-provisioning-policy-test)#
```

Related Commands

no	Removes an adopt rule

9.1.2 auto-create-rfd-template

auto-provisioning-policy

Enables auto creation of an RF Domain:

- when tokens are used to select the RF Domain to apply to devices matching the adoption criteria, and
- the token-specified RF Domain does not exist.

During device adoption, if the token-specified RF Domain (configured using the 'adopt' rule) is not found, the system auto creates a new RF Domain based on an existing RF Domain template specified using this command. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
auto-create-rfd-template <RF-DOMAIN-NAME>
```

Parameters

- `auto-create-rfd-template <RF-DOMAIN-NAME>`

auto-creates-rfd-template <RF-DOMAIN-NAME>	Auto creates a new RF Domain based on an existing RF Domain template • <RF-DOMAIN-NAME> – Specify the RF Domain name (should be existing and configured). The new RF Domain created is saved with the token name specified in the 'adopt' command. **Note:** For more information on configuring tokens, see *adopt*.

Example

The following example configures an adopt rule for adopting any AP7532 and applying an RF Domain matching the token "$MODEL[1:5]" to the adopted AP:

```
nx9500-6C8809(config-auto-provisioning-policy-test)#adopt ap7532 precedence 20
rf-domain $MODEL[1:5] any

nx9500-6C8809(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap7532 precedence 20 rf-domain $MODEL[1:5] any
nx9500-6C8809(config-auto-provisioning-policy-test)#
```

The following example enables auto creation of the following RF Domain using an existing RF Domain 'rfd-AP' as template:

- RF Domain name "AP-75": Applicable to any AP7532

```
nx9500-6C8809(config-auto-provisioning-policy-test)#auto-create-rfd-template rfd-
AP

nx9500-6C8809(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap7532 precedence 20 rf-domain $MODEL[1:5] any
 auto-create-rfd-template rfd-AP
nx9500-6C8809(config-auto-provisioning-policy-test)#
```

As per the above configurations, when an AP7532 comes up for first-time adoption, the system:

- Checks for an RF Domain matching the options provided in the ‘adopt’ rule, and if not found
- auto creates the RF Domain only if:
  - A token is specified in the ‘adopt’ rule. For example, $MODEL[1:5], and
  - the ‘auto-create-rfd-template’ option is configured
- Uses the ‘RF Domain’ specified in the auto-create-rfd-template command as a template. Therefore, the specified RF Domain should be existing and configured.
- Applies the new RF Domain to the AP.

Related Commands

no	Disables auto creation of an RF Domain

9.1.3 default-adoption

auto-provisioning-policy

Adopts devices, even when no matching rules are defined, and assigns a default profile and default RF Domain to the adopted device

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
default-adoption
```

Parameters

None

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#default-adoption

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt ap81xx precedence 1 profile default-ap81xx vlan 1
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands

no	Disables adoption of devices when matching rules are not found

9.1.4 deny

auto-provisioning-policy

Defines a deny device adoption rule

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
deny [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]

deny [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
[any|cdp-match|dhcp-option|fqdn|ip|ipv6|lldp-match|mac|model-number|serial-
number|vlan]

deny [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any

deny
[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|ap7602|
ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|nx5500|
nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> [cdp-match
<LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-
IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac
<START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number <SERIAL-
NUMBER>|vlan <VLAN-ID>]
```

Parameters

```
• deny[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|aap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any
```

deny	Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, VX9000, and NX9600 series. Note: 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type.
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence.
any	Indicates any device. Any device seeking adoption is denied adoption.

```
• deny[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-1000>
[cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-
IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-
STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-number
<SERIAL-NUMBER>|vlan <VLAN-ID>]
```

deny	Adds a deny adoption rule. The rule applies to the selected device types. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, VX9000, and NX9600.
precedence <1-10000>	Sets the rule precedence. A rule with a lower value has a higher precedence. After specifying the rule precedence, specify the match criteria. Devices matching the specified criteria are denied adoption.
cdp-match <LOCATION-SUBSTRING>	Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com, 'controller1', 'example', 'example.com', are examples of the substrings that will match. • <LOCATION-SUBSTRING> – Specify the value to match. Devices matching the specified value are denied adoption.
dhcp-option <DHCP-OPTION>	Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, for example 'tag1=value1;tag2=value2;tag3=value3'. The access point includes the value of tag 'rf-domain', if present. • <DHCP-OPTION> – Specify the DHCP option value to match. Devices matching the specified value are denied adoption.
fqdn <FQDN>	Matches a substring to the FQDN of a device (case insensitive) FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. • <FQDN> – Specify the FQDN. Devices matching the specified value are denied adoption.
ip [<START-IP> <END-IP>| <IP/MASK>]	Denies adoption if a device's IP address matches the specified IPv4 address or is within the specified IP address range • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Denies adoption if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IP address.

lldp-match <LLDP-STRING>	Matches a substring in a list of LLDP snoop strings (case insensitive). For example, if an access point snooped 3 devices: controller1.example.com, controller2.example.com and controller3.example.com,'controller1', 'example', 'example.com', are examples of the substrings that will match. LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the LLDP string. Devices matching the specified values are denied adoption.
mac <START-MAC> {<END-MAC>}	Denies adoption if a device's MAC address matches the specified MAC address or is within the specified MAC address range • <START-MAC> – Specify the first MAC address in the range. Provide this MAC address if you want to match for a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Denies adoption if a device's model number matches <MODEL-NUMBER> • <MODEL-NUMBER> – Specify the model number.
serial-number <SERIAL-NUMBER>	Denies adoption if a device's serial number matches <SERIAL-NUMBER> • <SERIAL-NUMBER> – Specify the serial number.
vlan <VLAN-ID>	Denies adoption if a device's VLAN matches <VLAN-ID> • <VLAN-ID> – Specify the VLAN ID.

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#deny ap71xx precedence 2
model-number AP7131N

rfs4000-229D58(config-auto-provisioning-policy-test)#deny ap71xx precedence 3 ip
192.168.13.23 192.168.13.23

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap81xx precedence 1 profile default-ap81xx vlan 1
 deny ap71xx precedence 2 model-number AP7131N
 deny ap71xx precedence 3 ip 192.168.13.23 192.168.13.23
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands

no	Removes a deny adoption rule

9.1.5 evaluate-always

auto-provisioning-policy

Sets flag to run this auto-provisioning policy every time an access point is adopted. The access point's previous adoption status is not taken into consideration.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
evaluate-always
```

Parameters

None

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#evaluate-always

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 evaluate-always
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands

no	Disables the running of this policy every time an AP is adopted

9.1.6 redirect

auto-provisioning-policy

Adds a rule redirecting device adoption to another controller within the system. Devices seeking adoption are redirected to a specified controller based on the redirection parameters specified.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
redirect[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
rfs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]

redirect [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
rfs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>] [any|cdp-match|dhcp-
option|fqdn|ip|ipv6|level|lldp-match|mac|model-number|pool|serial-number|vlan]

redirect [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
rfs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any

redirect[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
rfs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] [cdp-match
<LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-
IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|level [1|2]|lldp-match <LLDP-
STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|pool <1-2>|
serial-number <SERIAL-NUMBER>|vlan <VLAN-ID>] {upgrade}
```

Parameters

```
• redirect[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000>
controller [<CONTROLLER-IP>|<CONTROLLER-HOSTNAME>|ipv6] any
```

redirect	Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, VX9000, AP7632, AP7662, NX9600 series. Note: 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type. **Note:** An adoptee controller, such as RFS4000 and RFS6000 can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see *controller*.

precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
controller [<CONTROLLER-IP>| <CONTROLLER-HOSTNAME>|ipv6]	Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. • <CONTROLLER-IP> – Specifies the controller's IP address • <CONTROLLER-HOSTNAME> – Specifies the controller's hostname • ipv6 – Specify the controller's IPv6 address
any	Indicates any device. Any device seeking adoption is redirected.

```
• redirect [ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-1000>
controller [<CONTROLLER-IP>| <CONTROLLER-HOSTNAME>|ipv6] [cdp-match <LOCATION-
SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip [<START-IP> <END-IP>|<IP/
MASK>]|ipv6[<START-IP> <END-IP>|<IP/MASK>]|lldp-match <LLDP-STRING>|mac <START-
MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|pool <1-2>|serial-number <SERIAL-
NUMBER>|vlan <VLAN-ID>] {upgrade}
```

redirect	Adds a redirect adoption rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device type options are: anyap, AP6521, AP6522, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, VX9000, and NX9600. **Note:** An adoptee controller, such as RFS4000, RFS6000, and RFS7000, can be redirected to another controller (configured to adopt controllers) with a capacity equal to or higher than its own. For more information, see *controller*.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
controller [<CONTROLLER-IP>| <CONTROLLER-HOSTNAME>|ipv6]	Configures the controller to which the adopting devices are redirected. Specify the controller's IP address or hostname. • <CONTROLLER-IP> – Specifies the controller's IP address • <CONTROLLER-HOSTNAME> – Specifies the controller's hostname • ipv6 – Specify the controller's IPV6 address. After specifying the rule precedence and the controller, specify the match criteria.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are redirected.
dhcp-option <DHCP-OPTION>	Configures the DHCP options to match DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are redirected.

fqdn <FQDN>	Configures the FQDN to match FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. • <FQDN> – Specify the FQDN. Devices matching the specified value are redirected.
ip [<START-IP> <END-IP>| <IP/MASK>]	Configures a range of IP addresses and subnet address. Devices having IPv4 addresses within the specified range or are part of the specified subnet are redirected. • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
level[1|2]	Configures the routing level • level1 – Specifies level 1 as local routing • level2 – Specifies level2 as inter-site routing
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Redirects if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IP address.
lldp-match <LLDP-STRING>	Configures the device location to match, based on LLDP snoop strings LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the location. Devices matching the specified string are redirected.
mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are redirected. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are redirected.
pool <1-2>	Configures the controller pool • <1-2> – Configures the pool to which the specified controller belongs to. The default pool value is 1.
serial-number <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Devices matching the specified serial number are redirected.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are redirected.
upgrade	Optional. Upgrades APs before redirecting the device for adoption within the system

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 4
controller 192.168.13.10 ip 192.168.13.25 192.168.13.25

rfs4000-229D58(config-auto-provisioning-policy-test)#redirect ap81xx precedence 5
controller 192.168.13.10 model-number AP-8132-66040-US

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt ap81xx precedence 1 profile default-ap81xx vlan 1
 deny ap71xx precedence 2 model-number AP7131N
 deny ap71xx precedence 3 ip 192.168.13.23 192.168.13.23
 redirect ap81xx precedence 4 controller 192.168.13.10 ip 192.168.13.25
192.168.13.25
 redirect ap81xx precedence 5 controller 192.168.13.10 model-number AP-8132-66040-
US
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands

no	Removes a redirect rule

9.1.7 upgrade

auto-provisioning-policy

Adds a device upgrade rule to this auto provisioning policy. When applied to a controller, the upgrade rule ensures adopted devices, of the specified type, are upgraded automatically.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
upgrade[anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|r
fs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600]

upgrade [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
rfs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> [any|cdp-match|dhcp-option|fqdn|ip|ipv6|lldp-match|mac|model-number|
serial-number|vlan]

upgrade [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|rfs7000|
nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-10000> any

upgrade [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|ap7562|
ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|rfs6000|
rfs7000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip
[<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match
<LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-
number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

Parameters

```
• upgrade [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|
rfs6000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> any
```

upgrade	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, VX9000, and NX9600 series.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
any	Indicates any device. Any device, of the selected type, is upgraded.

```
• upgrade [anyap|ap6521|ap6522|ap6532|ap6562|ap71xx|ap7502|ap7522|ap7532|
ap7562|ap7602|ap7612|ap7622|ap7632|ap7662|ap81xx|ap82xx|ap8432|ap8533|rfs4000|
rfs6000|nx5500|nx7500|nx7510|nx7520|nx7530|nx9000|vx9000|nx9600] precedence <1-
10000> [cdp-match <LOCATION-SUBSTRING>|dhcp-option <DHCP-OPTION>|fqdn <FQDN>|ip
[<START-IP> <END-IP>|<IP/MASK>]|ipv6 [<START-IP> <END-IP>|<IP/MASK>]|lldp-match
<LLDP-STRING>|mac <START-MAC> {<END-MAC>}|model-number <MODEL-NUMBER>|serial-
number <SERIAL-NUMBER>|vlan <VLAN-ID>]
```

redirect	Adds a device upgrade rule. The rule applies to the device type selected. Specify the device type and assign a precedence to the rule. The different device types are: anyap, AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533, RFS4000, RFS6000, NX5500, NX75XX, NX95XX, VX9000, and NX9600 series. Note: 'anyap' is used in auto provisioning policies to create rules that are applicable to any AP regardless of the model type.
precedence <1-10000>	Sets the rule precedence. Rules with lower values get precedence over rules with higher values.
cdp-match <LOCATION-SUBSTRING>	Configures the device location to match, based on CDP snoop strings • <LOCATION-SUBSTRING> – Specify the location. Devices matching the specified string are upgraded.
dhcp-option <DHCP-OPTION>	Configures the DHCP options to match DHCP options identify the vendor and DHCP client functionalities. This information is used by the client to convey to the DHCP server that the client requires extra information in a DHCP response. • <DHCP-OPTION> – Specify the DHCP option value. Devices matching the specified value are upgraded.
fqdn <FQDN>	Configures the FQDN to match FQDN is a domain name that specifies its exact location in the DNS hierarchy. It specifies all domain levels, including its top-level domain and the root domain. • <FQDN> – Specify the FQDN. Devices matching the specified value are upgraded.
ip [<START-IP> <END-IP>| <IP/MASK>]	Configures a range of IP addresses and subnet address. Devices having IPv4 addresses within the specified range or are part of the specified subnet are upgraded. • <START-IP> – Specify the first IPv4 address in the range. • <END-IP> – Specify the last IPv4 address in the range. • <IP/MASK> – Specify the IPv4 subnet and mask to match against the device's IP address.
ipv6 [<START-IP> <END-IP>| <IP/MASK>]	Upgrades if a device's IPv6 address matches the specified IP address or is within the specified IP address range • <START-IP> – Specify the first IPv6 address in the range. • <END-IP> – Specify the last IPv6 address in the range. • <IP/MASK> – Specify the IPv6 subnet and mask to match against the device's IP address.

lldp-match <LLDP-STRING>	Configures the device location to match, based on LLDP snoop strings LLDP is a vendor neutral link layer protocol used to advertise a network device's identity, capabilities, and neighbors on a local area network. • <LLDP-STRING> – Specify the location. Devices matching the specified string are upgraded.
mac <START-MAC> {<END-MAC>}	Configures a single or a range of MAC addresses. Devices matching the specified values are upgraded. • <START-MAC> – Specify the first MAC address in the range. Provide only this MAC address to filter a single device. • <END-MAC> – Optional. Specify the last MAC address in the range.
model-number <MODEL-NUMBER>	Configures the device model number • <MODEL-NUMBER> – Specify the model number. Devices matching the specified model number are upgraded.
serial-number <SERIAL-NUMBER>	Configures the device's serial number • <SERIAL-NUMBER> – Specify the serial number. Devices matching the specified serial number are upgraded.
vlan <VLAN-ID>	Configures the VLAN ID • <VLAN-ID> – Specify the VLAN ID. Devices assigned to the specified VLAN are upgraded.

Example

```
rfs4000-229D58(config-auto-provisioning-policy-test)#upgrade ap6521 precedence 1
any

rfs4000-229D58(config-auto-provisioning-policy-test)#upgrade rfs4000 precedence 2
ip 192.168.13.1 192.168.13.5

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 upgrade ap6521 precedence 1 any
 upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

Related Commands

no	Removes an upgrade rule

9.1.8 no

auto-provisioning-policy

Removes a deny, permit, or redirect rule from the specified auto provisioning policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [adopt|auto-create-rfd-template|default-adoption|deny|evaluate-always|
redirect|upgrade]
no adopt precedence <1-10000>
no auto-create-rfd-template
no deny precedence <1-10000>
no evaluate-always
no default-adoption
no redirect precedence <1-10000>
no upgrade precedence <1-10000>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny, permit, or redirect rule from the specified auto provisioning policy

Example

The following example shows the auto-provisioning-policy 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 default-adoption
 adopt ap81xx precedence 1 profile default-ap81xx vlan 1
 deny ap71xx precedence 2 model-number AP7131N
 deny ap71xx precedence 3 ip 192.168.13.23 192.168.13.23
 redirect ap81xx precedence 4 controller 192.168.13.10 ip 192.168.13.25
192.168.13.25
 redirect ap81xx precedence 5 controller 192.168.13.10 model-number AP-8132-66040-
US
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#no default-adoption
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 2
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 3
rfs4000-229D58(config-auto-provisioning-policy-test)#no deny precedence 5
```

The following example shows the auto-provisioning-policy 'test' settings after the 'no' commands are executed:

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 adopt ap81xx precedence 1 rf-domain TechPubs vlan 1
 redirect ap81xx precedence 4 controller 192.168.13.10 ip 192.168.13.25
192.168.13.25
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

```
rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 upgrade ap6521 precedence 1 any
 upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#

rfs4000-229D58(config-auto-provisioning-policy-test)#no upgrade precedence 1

rfs4000-229D58(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
 upgrade rfs4000 precedence 2 ip 192.168.13.1 192.168.13.5
rfs4000-229D58(config-auto-provisioning-policy-test)#
```

10 ASSOCIATION-ACL-POLICY

This chapter summarizes the association ACL policy commands in the CLI command structure. An association ACL is a policy-based *Access Control List* (ACL) that either *allows* or *denies* wireless clients from connecting to a wireless controller, service platform, or access point managed WLAN.

System administrators can use an association ACL to grant or restrict wireless clients access to the WLAN by specifying a client's MAC address or a range of MAC addresses to either include or exclude from WLAN connectivity. Association ACLs are applied to WLANs as an additional access control mechanism.

Use the (config) instance to configure the association ACL policy. To navigate to the association-acl-policy instance, use the following commands:

```
<DEVICE>(config)#association-acl-policy <POLICY-NAME>

rfs6000-37FABE(config)#association-acl-policy test
rfs6000-37FABE(config-assoc-acl-test)#

rfs6000-37FABE(config-assoc-acl-test)#?
Association ACL Mode commands:
  deny      Specify MAC addresses to be denied
  no        Negate a command or set its defaults
  permit    Specify MAC addresses to be permitted

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-37FABE(config-assoc-acl-test)#
```

NOTE: If creating an new association ACL policy, provide a name specific to its function. Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.

Before defining an association ACL policy and applying it to a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The name and configuration of an association ACL policy should meet the requirements of the WLANs it may map to. However, be careful not to name ACLs after specific WLANs, as individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a layer 2 interface. If a MAC ACL is already configured on a layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

10.1 association-acl-policy

- *ASSOCIATION-ACL-POLICY*

The following table summarizes association ACL policy configuration commands:

Table 10.1 *Association-ACL-Policy-Config Commands*

Command	Description	Reference
deny	Specifies a range of MAC addresses denied access to the WLAN	*page 10-3*
no	Removes a deny or permit rule from this association ACL policy	*page 10-5*
permit	Specifies a range of MAC addresses allowed access to the WLAN	*page 10-6*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

10.1.1 deny

association-acl-policy

Creates a list of devices denied access to the managed network. Devices are identified by their MAC address. A single MAC address or a range of MAC addresses can be denied access. This command also sets the precedence on how deny rules are applied. Up to a thousand (1000) deny rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and is applied to packets on the basis of the precedence value. Lower the precedence, higher is the priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, prioritize ACLs accordingly as they are added.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
deny <STARTING-MAC> [<ENDING-MAC>|precedence]

deny <STARTING-MAC> precedence <1-1000>
deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

Parameters

- `deny <STARTING-MAC> precedence <1-1000>`

deny	Adds a single device or a set of devices to the deny list
<STARTING-MAC>	To add a single device, enter its MAC address in the <STARTING-MAC> parameter.
precedence <1-1000>	Sets a precedence rule. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a precedence value from 1 - 1000.

- `deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>`

deny	Adds a single device or a set of devices to the deny list To add a set of devices, provide the range of MAC addresses.
<STARTING-MAC>	Specify the first MAC address in the range.
<ENDING-MAC>	Specify the last MAC address in the range.
precedence <1-1000>	Sets a precedence rule. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

Usage Guidelines

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are applied in an increasing order of precedence. That means the rule with precedence 1 is applied first, then the rule with precedence 2 and so on.

Example

```
rfs6000-37FABE(config-assoc-acl-test)#deny 11-22-33-44-55-01 11-22-33-44-55-FF
precedence 150

rfs6000-37FABE(config-assoc-acl-test)#deny 11-22-33-44-56-01 11-22-33-44-56-01
precedence 160

rfs6000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160
rfs6000-37FABE(config-assoc-acl-test)#
```

Related Commands

no	Removes a deny rule based on its precedence value

10.1.2 no

association-acl-policy

Removes a deny or permit rule from this association ACL policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [deny|permit]

no deny <STARTING-MAC> precedence <1-1000>
no deny <STARTING-MAC> <ENDING-MAC> precedence <1-1000>

no permit <STARTING-MAC> precedence <1-1000>
no permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny or permit rule from this association ACL policy

Example

The following example shows the association ACL policy 'test' settings before the 'no' commands is executed:

```
rfs6000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 deny 11-22-33-44-56-01 11-22-33-44-56-01 precedence 160
rfs6000-37FABE(config-assoc-acl-test)#

rfs6000-37FABE(config-assoc-acl-test)#no deny 11-22-33-44-56-01 11-22-33-44-56-FF
precedence 160
```

The following example shows the association ACL policy 'test' settings after the 'no' commands is executed:

```
rfs6000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
rfs6000-37FABE(config-assoc-acl-test)#
```

10.1.3 permit

association-acl-policy

Creates a list of devices allowed access to the managed network. Devices are permitted access based on their MAC address. A single MAC address or a range of MAC addresses can be specified. This command also sets the precedence on how permit list rules are applied. Up to a thousand (1000) permit rules can be defined for every association ACL policy. Each rule has a unique sequential precedence value assigned, and are applied to packets on the basis of this precedence value. Lower the precedence of a rule, higher is its priority. This results in the rule with the lowest precedence being applied first. No two rules can have the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
permit <STARTING-MAC> [<ENDING-MAC>|precedence]

permit <STARTING-MAC> precedence <1-1000>
permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>
```

Parameters

- `permit <STARTING-MAC> precedence <1-1000>`

permit	Adds a single device or a set of devices to the permit list
<STARTING-MAC>	To add a single device, enter its MAC address in the <STARTING-MAC> parameter.
precedence <1-1000>	Specifies a rule precedence. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

- `permit <STARTING-MAC> <ENDING-MAC> precedence <1-1000>`

permit	Adds a single device or a set of devices to the permit list To add a set of devices, provide the MAC address range.
<STARTING-MAC>	Specify the first MAC address of the range.
<ENDING-MAC>	Specify the last MAC address of the range.
precedence <1-1000>	Specifies a rule precedence. Rules are applied in an increasing order of precedence. • <1-1000> – Specify a value from 1 - 1000.

Usage Guidelines

Every rule has a unique sequential precedence value. You cannot add two rules with the same precedence. Rules are applied to packets in an increasing order of precedence. That means the rule with precedence 1 is applied first, then the rule with precedence 2 and so on.

Example

```
rfs6000-37FABE(config-assoc-acl-test)# permit 11-22-33-44-66-01 11-22-33-44-66-FF
precedence 170

rfs6000-37FABE(config-assoc-acl-test)# permit 11-22-33-44-67-01 precedence 180

rfs6000-37FABE(config-assoc-acl-test)#show context
association-acl-policy test
 deny 11-22-33-44-55-01 11-22-33-44-55-FF precedence 150
 permit 11-22-33-44-66-01 11-22-33-44-66-FF precedence 170
 permit 11-22-33-44-67-01 11-22-33-44-67-01 precedence 180
rfs6000-37FABE(config-assoc-acl-test)#
```

Related Commands

no	Removes a permit rule based on its precedence

11 ACCESS-LIST

This chapter summarizes IPv4, IPv6, and MAC access list commands in the CLI command structure.

Access lists control access to the managed network using a set of rules also known as *Access Control Entries* (ACEs). Each rule specifies an action taken when a packet matches that rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. A set of deny and/or permit rules based on IP (IPv4 and IPv6) addresses constitutes a IP *Access Control List* (ACL). Similarly, a set of deny and/or permit rules based on MAC addresses constitutes a MAC ACL.

Within a managed network, IP ACLs are used as firewalls to filter packets and also mark packets. IP based firewall rules are specific to the source and destination IP addresses and have unique precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying an IP ACL. With either IPv4 or IPv6, create access rules for traffic entering a controller, service platform, or access point interface, because if you are going to deny specific types of packets, it's recommended you do it before the controller, service platform, or access point spends time processing them, since access rules are given priority over other types of firewall rules.

MAC ACLs are firewalls that filter or mark packets based on the MAC address which they arrive, as opposed to filtering packets on layer 2 ports. Optionally filter layer 2 traffic on a physical layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to controller managed packet traffic.

Once defined, an IP and/or MAC ACL (consisting of a set of firewall rules) must be applied to an interface to be a functional filtering tool.

Firewall supported devices (access points, wireless controllers, and service platforms) process firewall rules (within an IP/MAC ACL) sequentially, in ascending order of their precedence value. When a packet matches a rule, the firewall applies the action specified in the rule to determine whether the traffic is allowed or denied. Once a match is made, the firewall does not process subsequent rules in the ACL.

The WiNG software enables the configuration of IP SNMP ACLs. These ACLs control access by combining IP ACLs with SNMP server community strings.

The following ACLs are supported:

- *ip-access-list*
- *mac-access-list*
- *ipv6-access-list*
- *ip-snmp-access-list*
- *ex3500-ext-access-list*
- *ex3500-std-access-list*

Use IP and MAC commands under the global configuration to create an access list.

- When the access list is applied on an Ethernet port, it becomes a port ACL.
- When the access list is applied on a VLAN interface, it becomes a router ACL.

Use the (config) instance to configure a new ACL or modify an existing ACL. To navigate to the (config-access-list) instance, use the following commands:

```
<DEVICE>(config)#ip access-list <IP-ACCESS-LIST-NAME>

<DEVICE>(config)#mac access-list <MAC-ACCESS-LIST-NAME>

<DEVICE>(config)#ipv6 access-list <IPv6-ACCESS-LIST-NAME>

<DEVICE>(config)#ip snmp-access-list <SNMP-ACCESS-LIST-NAME>

<DEVICE>(config)#ex3500-ext-access-list <EX3500-EXT-ACCESS-LIST-NAME>

<DEVICE>(config)#ex3500-std-access-list <EX3500-STD-ACCESS-LIST-NAME>
```

NOTE: If creating an new ACL policy, provide a name that uniquely identifies its purpose. The name cannot exceed 32 characters.

ip-access-list

```
rfs6000-37FABE(config)#ip access-list test
rfs6000-37FABE(config-ip-acl-test)#?
ACL Configuration commands:
  deny      Specify packets to reject
  disable   Disable rule if not needed
  insert    Insert this rule (instead of overwriting a existing rule)
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-37FABE(config-ip-acl-test)#
```

mac-access-list

```
rfs6000-37FABE(config)#mac access-list test
rfs6000-37FABE(config-mac-acl-test)#?
MAC Extended ACL Configuration commands:
  deny      Specify packets to reject
  disable   Disable rule if not needed
  ex3500    EX3500 device
  insert    Insert this rule (instead of overwriting a existing rule)
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  do        Run commands from Exec mode
  commit    Commit all changes made in this session
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal
```

```
rfs6000-37FABE(config-mac-acl-test)#
```

ipv6-access-list

```
rfs6000-37FABE(config-ipv6-acl-test)#?
IPv6 Access Control Mode commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-37FABE(config-ipv6-acl-test)#
```

ip-snmp-access-list

```
nx9500-6C8809(config-ip-snmp-acl-test)#?
SNMP ACL Configuration commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

nx9500-6C8809(config-ip-snmp-acl-test)#
```

The WiNG NOC controller also has the capabilities of adopting and managing EX3500 series switch. These switches are Gigabit Ethernet layer 2 switches with either 24 or 48 10/100/1000-BASE-T ports, and four *Small Form Factor Pluggable* (SFP) transceiver slots for fiber connectivity. Once adopted to the NOC, various ACLs specifically defined for a **EX3500** switch can be used to either prevent or allow specific clients from using it.

The following EX3500 ACLs are supported:

- *ex3500-ext-access-list*
- *ex3500-std-access-list*
- *ex3500*: This configures a EX3500 deny or permit rule in a MAC ACL.

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

11.1 ip-access-list

ACCESS-LIST

The following table summarizes IP access list configuration commands:

Table 11.1 *IP-Access-List-Config Commands*

Command	Description	Reference
deny	Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined for specified address(es).	*page 11-5*
disable	Disables an existing deny or permit rule without removing it from the ACL	*page 11-17*
insert	Inserts a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence	*page 11-20*
no	Removes a deny and/or a permit access rule from a IP ACL	*page 11-22*
permit	Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined for specified address(es).	*page 11-23*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

11.1.1 deny

ip-access-list

Creates a deny rule that rejects packets from a specified source IP and/or to a specified destination IP. You can also use this command to modify an existing deny rule.

NOTE: Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
deny [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]

deny <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-
HOST-IP>|<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}

deny dns-name [contains|exact|suffix]

deny dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}

deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-
HOST-IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-
description <LINE>)}

deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host
<SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-
IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host
<SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-
IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-
ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq
<SOURCE-PORT>|host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq [<1-65535>|
<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|
ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-precedence <1-
5000>) {(rule-description <LINE>)}
```

Parameters

```
• deny <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-
NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host
<DEST-HOST-IP>|<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<NETWORK-SERVICE-ALIAS-NAME>	Applies this deny rule to packets based on service protocols and ports specified in the network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL deny rule. **Note:** For more information on configuring network-service alias, see *alias*.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).
any	Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are dropped.
any	Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are dropped.

host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

• `deny dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>) {(rule-description <LINE>)}`

dns-name	Applies this deny rule to packets based on dns-names specified in the network-service
contains	Matches any hostname which has this DNS label. (for example, *.test.*)
exact	Matches an exact hostname as specified in the network-service
suffix	Matches any hostname as suffix (for example, *.test)
<WORD>	Identifies a specific host (as the source to match) by its domain name. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are dropped.
log	Logs all deny events matching this dns entry. If a dns-name is matched an event is logged.

rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

• `deny icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-NAME>|any|host <DEST-HOST-IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>)` *`{(rule-description <LINE>)}`*

icmp	Applies this deny rule to *Internet Control Message Protocol* (ICMP) packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. ICMP packets received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the destination as any IP address. ICMP packets addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.

<ICMP-TYPE>	Defines the ICMP packet type For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.
<ICMP-CODE>	Defines the ICMP message type For example, an ICMP code 3 indicates “Destination Unreachable”, code 1 indicates “Host Unreachable”, and code 3 indicates “Port Unreachable.” **Note:** After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match.
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• deny ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-
HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

ip	Applies this deny rule to IP packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. IP packets received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host’s exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are dropped.
any	Specifies the destination as any IP address. IP packets addressed to any destination are dropped.

host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|
host <DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

proto	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter
<PROTOCOL-NUMBER>	Filters protocols using their *Internet Assigned Numbers Authority* (IANA) protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the *Enhanced Internet Gateway Routing Protocol* (EIGRP) protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.
gre	Identifies the *General Routing Encapsulation* (GRE) protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.

igmp	Identifies the *Internet Group Management Protocol* (IGMP) protocol (number 2) IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.
igp	Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used *interior gateway protocol* (IGP) protocols are: *Routing Information Protocol* (RIP) and *Open Shortest Path First* (OSPF)
ospf	Identifies the OSPF protocol (number 89) OSPF is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.
vrrp	Identifies the *Virtual Router Redundancy Protocol* (VRRP) protocol (number 112) VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are dropped.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are dropped. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are dropped. • <VLAN-ID> – Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are dropped.

any	Specifies the destination as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are dropped. • <SOURCE-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are dropped. • <NETWORK-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). **Note:** After specifying the source and destination IP address(es), specify the action taken in case of a match.
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• deny [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|eq <SOURCE-PORT>|host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq [<1-
65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|
sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-precedence
<1-5000>) {(rule-description <LINE>)}
```

tcp	Applies this deny rule to TCP packets only
udp	Applies this deny rule to UDP packets only
<SOURCE-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are dropped.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are dropped. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.

any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IP address. TCP/UDP packets received from any source are dropped.
from-vlan <VLAN-ID>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are dropped. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are dropped.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are dropped.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are dropped. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.

eq [<1-65535>| <SERVICE-NAME>| |bgp|dns|ftp| ftp-data|gropher| https|ldap|nntp|ntp| pop3|sip|smtp| ssh|telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated *Border Gateway Protocol* (BGP) protocol port (179) • dns – The designated *Domain Name System* (DNS) protocol port (53) • ftp – The designated *File Transfer Protocol* (FTP) protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated *Lightweight Directory Access Protocol* (LDAP) protocol port (389) • nntp – The designated *Network News Transfer Protocol* (NNTP) protocol port (119) • ntp – The designated *Network Time Protocol* (NTP) protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated *Session Initiation Protocol* (SIP) protocol port (5060) • smtp – The designated *Simple Mail Transfer Protocol* (SMTP) protocol port (25) • ssh – The designated *Secure Shell* (SSH) protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated *Trivial File Transfer Protocol* (TFTP) protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all deny events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- IP
- ICMP
- TCP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last *access control entry* (ACE) in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria
- Select ICMP as the protocol to allow or deny ICMP packets. Selecting ICMP filters ICMP packets based on ICMP type and code.

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example

```
rfs6000-37FABE(config-ip-acl-test)#deny proto vrrp any any log rule-precedence 600

rfs6000-37FABE(config-ip-acl-test)#deny proto ospf any any log rule-precedence 650

rfs6000-37FABE(config-ip-acl-test)#show context
ip access-list test
 deny proto vrrp any any log rule-precedence 600
 deny proto ospf any any log rule-precedence 650
rfs6000-37FABE(config-ip-acl-test)#
```

Using aliases in IP access list.

The following examples show the usage of network-group aliases:

```
rfs4000-229D58(config)#ip access-list bar
```

Example 1:

```
rfs4000-229D58(config-ip-acl-bar)#permit ip $foo any rule-precedence 10
```

Example 2

```
rfs4000-229D58(config-ip-acl-bar)#permit tcp 192.168.100.0/24 $foobar eq ftp rule-precedence 20
```

Example 3

```
rfs4000-229D58(config-ip-acl-bar)#deny ip $guest  $lab rule-precedence 30
```

- In example1, network-group alias $foo is used as a source
- In example 2, network-group alias $foobar is used as a destination
- In example 3, network-group aliases $guest and $lab are used as source and destination respectively.

The following examples show the usage of network-service aliases:

Example 4

```
rfs4000-229D58(config-ip-acl-bar)# permit $kerberos 10.60.20.0/24 $kerberos-servers log rule-precedence 40
```

Example 5

```
rfs4000-229D58(config-ip-acl-bar)#permit $Tandem 10.60.20.0/24 $Tandem-servers log rule-precedence 50
```

In examples 4, and 5:

- The network-service aliases ($kerberos and $Tandem) define the destination protocol-port combinations
- The source network is 10.60.20.0/24
- The destination network-address combinations are defined by the network-group aliases ($kerberos-servers and $Tandem-servers)

Related Commands

no	Removes a specified IP deny access rule
alias	Creates and configures aliases (network, VLAN, and service)

11.1.2 disable

ip-access-list

Disables an existing deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
disable [deny|insert|permit]

disable [deny|insert [deny|permit]|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]

disable [deny|insert [deny|permit]|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name [contains|exact|suffix]|icmp|ip|proto <PROTOCOL-OPTIONS>|tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence)
```

Parameters

```
• disable [deny|insert [deny|permit]|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name [contains|exact|suffix]|icmp|ip|proto <PROTOCOL-OPTIONS>|tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-IP>] (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence)
```

disable [deny|insert [deny|permit]|permit]	Disables a deny or permit access rule without removing it from the ACL This command also enables the insertion of a disable deny or permit rule without overwriting an existing rule in the IP ACL. **Note:** To disable an existing deny/permit rule, provide the exact values used to configure the deny or permit rule.
<NETWORK-SERVICE-ALIAS-NAME>	Specifies the network-service alias, identified by the <NETWORK-SERVICE-ALIAS-NAME> keyword, associated with the deny/permit rule
dns-name [contains|exact|suffix]	Specifies the packets to reject based on the dns-name match. Applies this deny rule to packets based on dns-names specified in the network-service
icmp	Disables a rule applicable to ICMP packets only
ip	Disables a rule applicable to IP packets only
proto <PROTOCOL-OPTIONS>	Disables a rule applicable to any Internet protocol other than TCP, UDP, or ICMP packets • <PROTOCOL-OPTIONS> – Identify the Internet protocol using the options available.
tcp	Disables a rule applicable to TCP packets only

udp	Disables a rule applicable to UDP packets only **Note:** After specifying the packet type, specify the source and destination devices and network address(es) to match.
<SOURCE-IP/MASK>	Specify the source IP address and mask in the A.B.C.D/M format.
<NETWORK-GROUP-ALIAS-NAME>	Specifies the network-group alias, identified by the <NETWORK-GROUP-ALIAS-NAME> keyword, associated with this deny/permit rule
any	Select 'any' if the rule is applicable to any source IP address.
from-vlan <VLAN-ID>	Specify the VLAN IDs.
host <SOURCE-HOST-IP>	Specify the source host's exact IP address.
<DEST-IP/MASK>	Specify the destination IP address and mask in the A.B.C.D/M format.
<NETWORK-GROUP-ALIAS-NAME>	Specifies the network-group alias, identified by the <NETWORK-GROUP-ALIAS-NAME> keyword, associated with this deny/permit rule
any	Select 'any' if the rule is applicable to any destination IP address.
host <DEST-HOST-IP>	Specify the destination host's exact IP address.
log	Select log, if the rule has been configured to log records in case of a match.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000>	Specify the rule precedence. The deny or permit rule with the specified precedence is disabled. **Note:** To enable a disabled rule, enter the rule again without the 'disable' keyword. **Note:** The *no > disable* command removes a disabled rule from the ACL.

Example

The following example shows the 'auto-tunnel-acl' settings before the disable command is executed:

```
rfs6000-37FABE(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
 permit ip host 200.200.200.99 any rule-precedence 3
rfs6000-37FABE(config-ip-acl-auto-tunnel-acl)#

rfs6000-37FABE(config-ip-acl-auto-tunnel-acl)#disable permit ip host
200.200.200.99 any rule-precedence 3
rfs6000-37FABE(config-ip-acl-auto-tunnel-acl)#
```

The following example shows the 'auto-tunnel-acl' settings after the disable command is executed:

```
rfs6000-37FABE(config-ip-acl-auto-tunnel-acl)#show context
ip access-list auto-tunnel-acl
 permit ip host 200.200.200.99 30.30.30.1/24 rule-precedence 2
```

```
 disable permit ip host 200.200.200.99 any rule-precedence 3
rfs6000-37FABE(config-ip-acl-auto-tunnel-acl)#

rfs4000-229D58(config-ip-acl-test)#deny icmp any any log rule-precedence 1

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#

rfs4000-229D58(config-ip-acl-test)#disable deny icmp any any rule-precedence 1

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 disable deny icmp any any rule-precedence 1
rfs4000-229D58(config-ip-acl-test)#

In the following example a disable deny rule has been inserted in the IP ACL "test":

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#

rfs4000-229D58(config-ip-acl-test)#disable insert deny ip any any log rule-
precedence 2

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 disable deny ip any any log rule-precedence 2
 permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#
```

Related Commands

no	Enables a disabled deny or permit rule
deny	Creates a new deny access rule or modifies an existing rule
permit	Creates a new permit access rule or modifies an existing rule
alias	Creates and configures a aliases (network, VLAN, and service)

11.1.3 insert

ip-access-list

Enables the insertion of a rule in an IP ACL without overwriting or replacing an existing rule having the same precedence

The insert option allows a new rule to be inserted within a IP access list. Consider an IP ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule's precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.

NOTE: NOT using *insert* when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],rule-
precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• insert [deny|permit] <PARAMETERS> (log,mark [8021p <0-7>|dscp <0-63>],rule-
precedence <1-5000>) {(rule-description <LINE>)}
```

[deny|permit]	Inserts a deny or a permit rule within an IP ACL
<PARMETERS>	Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see *deny*. For more information on the permit rule, see *permit*.
log	After specifying the match criteria, specify the action taken for filtered packets Logs all deny/permit events matching this entry. If a source and/or destination IP address is matched an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header

rule-precedence <1-5000> rule-description <LINE>	Assigns a precedence for this deny/permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this new rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet that matches the entry sent to the console.

Example

```
rfs4000-229D58(config-ip-acl-test)#deny tcp from-vlan 1 any any rule-precedence 1

rfs4000-229D58(config-ip-acl-test)#permit icmp any host 192.168.13.7 1 1 rule-
precedence 2

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 permit icmp any host 192.168.13.7 1 1 rule-precedence 2
rfs4000-229D58(config-ip-acl-test)#

In the following example a new rule is inserted between the rules having precedences
1 and 2. The precedence of the existing precedence '2' rule changes to precedence 3.

rfs4000-229D58(config-ip-acl-test)#insert deny ip any any rule-precedence 2

rfs4000-229D58(config-ip-acl-test)#show context
ip access-list test
 deny tcp from-vlan 1 any any rule-precedence 1
 deny ip any any rule-precedence 2
 permit icmp any host 192.168.13.7 1 1 rule-precedence 3
rfs4000-229D58(config-ip-acl-test)#
```

Related Commands

alias	Creates and configures aliases (network, VLAN, and service)

11.1.4 no

ip-access-list

Removes a deny, permit, or disable rule

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [deny|disable|permit]

no [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]
<RULE-PARAMETERS>

no disable [deny|permit] [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|
tcp|udp] <RULE-PARAMETERS>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny, permit, or disable rule

Usage Guidelines

Removes an access list control entry. Provide the rule-precedence value when using the no command.

Example

The following example shows the ACL ‘test’ settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-ip-acl-test)#show context
ip access-list test
 deny proto vrrp any any log rule-precedence 600
 deny proto ospf any any log rule-precedence 650
rfs6000-37FABE(config-ip-acl-test)#

rfs6000-37FABE(config-ip-acl-test)#no deny proto vrrp any any rule-precedence 600
rfs6000-37FABE(config-ip-acl-test)#no deny proto ospf any any rule-precedence 650
```

The following example shows the ACL ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-ip-acl-test)#show context
ip access-list test
rfs6000-37FABE(config-ip-acl-test)#
```

11.1.5 permit

ip-access-list

Creates a permit rule that marks packets (from a specified source IP and/or to a specified destination IP) for forwarding. You can also use this command to modify an existing permit rule.

NOTE: Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for IP ACLs provides the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
permit [<NETWORK-SERVICE-ALIAS-NAME>|dns-name|icmp|ip|proto|tcp|udp]

permit <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|
any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host <DEST-
HOST-IP>|<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}

permit dns-name [contains|exact|suffix]

permit dns-name [contains|exact|suffix] <WORD> (log,rule-precedence <1-5000>)
{(rule-description <LINE>)}

permit dns-name exact <WORD> (log,mark [8021p <0-7>|dscp <0-63>],rule-precedence
<1-5000>) {(rule-description <LINE>)}

permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-
HOST-IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-
description <LINE>)}

permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-
HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host
<SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-
IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

permit [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan
<VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-
NAME>|any|eq <SOURCE-PORT>|host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq
[<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|
sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-precedence
<1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• permit <NETWORK-SERVICE-ALIAS-NAME> [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-
NAME>|any|from-vlan <VLAN-ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|any|host
<DEST-HOST-IP>|<NETWORK-GROUP-ALIAS-NAME>] (log,mark [8021p <0-7>|dscp <0-63>],
rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<NETWORK-SERVICE-ALIAS-NAME>	Applies this permit rule to packets based on service protocols and ports specified in the network-service alias • <NETWORK-SERVICE-ALIAS-NAME> – Specify the network-service alias name (should be existing and configured). A network-service alias defines service protocols and ports to match. When used with an ACL, the network-service alias defines the service-specific components of the ACL permit rule. **Note:** For more information on configuring network-service alias, see *alias*.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified network are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, received from the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). A network-group alias defines a single or a range of addresses of devices, hosts, and networks. When used with an ACL, the network-group alias defines the network-specific component of the ACL rule (permit/deny).
any	Specifies the source as any source IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified VLAN(s) are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified network are permitted.
any	Specifies the destination as any destination IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to any destination are permitted.

host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets, matching the service protocols and ports specified in the network-service alias, addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. Packets, matching the service protocols and ports specified in the network-service alias, destined for the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. if any specified type of packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

- `permit dns-name [contains|exact (mark)|suffix] <WORD> (log,rule-precedence <1-5000>) {(rule-description <LINE>)}`

dns-name	Applies this permit rule to packets based on dns-names specified in the network-service
contains	Matches any hostname which has this DNS label. (for example, *.test.*)
exact	Matches an exact hostname as specified in the network-service
suffix	Matches any hostname as suffix (for example, *.test)
<WORD>	Identifies a specific host (as the source to match) by its domain name. Packets, matching the service protocols and ports specified in the network-service alias, received from the specified host are forwarded.
log	Logs all permit events matching this dns entry. If a dns-name is matched an event is logged.
mark [8021p <0-7>| dscp <0-63>]	Specifies packets to mark • 8021p <0-7> – Marks packets by modifying 802.1.p VLAN user priority • dscp <0-63> – Marks packets by modifying DSCP TOS bits in the header

rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• permit icmp [<SOURCE-IP/MASK>|<NETWORK-GROUP-NAME>|any|from-vlan <VLAN-ID>|
host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-NAME>|any|host <DEST-HOST-
IP>] (<ICMP-TYPE> <ICMP-CODE>,log,rule-precedence <1-5000>) {(rule-description
<LINE>)}
```

icmp	Applies this permit rule to ICMP packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. ICMP packets received from the specified sources are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. ICMP packets received from the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any source IP address. ICMP packets received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. ICMP packets received from the VLANs identified here are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. ICMP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. ICMP packets addressed to specified destinations are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. ICMP packets destined for addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the destination as any destination IP address. ICMP packets addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. ICMP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.

<ICMP-TYPE>	Defines the ICMP packet type For example, an ICMP type 0 indicates it is an ECHO REPLY, and type 8 indicates it is an ECHO.
<ICMP-CODE>	Defines the ICMP message type For example, an ICMP code 3 indicates “Destination Unreachable”, code 1 indicates “Host Unreachable”, and code 3 indicates “Port Unreachable.” **Note:** After specifying the source and destination IP address(es), the ICMP message type, and the ICMP code, specify the action taken in case of a match.
log	Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a ICMP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• permit ip [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-
ID>|host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host
<DEST-HOST-IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

ip	Applies this permit rule to IP packets only
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. IP packets received from the specified networks are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets received from the addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any source IP address. IP packets received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. IP packets received from the specified VLANs are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLAN IDs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. IP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host’s exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. IP packets addressed to the specified networks are permitted.

any	Specifies the destination as any destination IP address. IP packets addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. IP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. IP packets destined for addresses identified by the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
log	Logs all permit events matching this entry. If a source and/or destination IP address is matched (i.e. a IP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igmp|igp|ospf|vrrp]
[<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID>|host
<SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|host <DEST-HOST-
IP>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

proto	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.
<PROTOCOL-NUMBER>	Filters protocols using their IANA protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.
gre	Identifies the GRE protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.

igmp	Identifies the IGMP protocol (number 2) IGMP establishes and maintains multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.
igp	Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used *interior gateway protocol* (IGP) protocols are: *Routing Information Protocol* (RIP) and *Open Shortest Path First* (OSPF)
ospf	Identifies the OSPF protocol (number 89) OSPF is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.
vrrp	Identifies the VRRP protocol (number 112) VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
<SOURCE-IP/MASK>	Specifies the source IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified sources are permitted.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the source IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the sources defined in the network-group alias are permitted. • <NETWORK-GROUP-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured).
any	Specifies the source as any IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are permitted.
from-vlan <VLAN-ID>	Specifies a single VLAN or a range of VLANs as the match criteria. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the VLANs identified here are permitted. • <VLAN-ID> – Specify the VLAN ID. A range of VLANs is represented by the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	Specifies the destination IP address and mask (A.B.C.D/M) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified destinations are permitted.

any	Specifies the destination as any destination IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are permitted.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addresses to the specified host are permitted. • <SOURCE-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	Applies a network-group alias to identify the destination IP addresses. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the destinations identified in the network-group alias are permitted. • <NETWORK-ALIAS-NAME> – Specify the network-group alias name (should be existing and configured). **Note:** After specifying the source and destination IP address(es), specify the action taken in case of a match.
log	Logs all deny events matching this entry. If a source and/or destination IP address is matched (i.e. a packet (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

• `permit [tcp|udp] [<SOURCE-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|from-vlan <VLAN-ID> |host <SOURCE-HOST-IP>] [<DEST-IP/MASK>|<NETWORK-GROUP-ALIAS-NAME>|any|eq <SOURCE-PORT> |host <DEST-HOST-IP>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>)` *`{(rule-description <LINE>)}`*

tcp	Applies this permit rule to TCP packets only
udp	Applies this deny rule to UDP packets only
<SOURCE-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source IP address and mask (A.B.C.D/M) to match. TCP/UDP packets received from the specified sources are permitted.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the source IP addresses. TCP/UDP packets received from the VLANs identified here are permitted. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured). After specifying the source and destination IP address(es), specify the action taken in case of a match.

any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any source IP address. TCP/UDP packets received from any source are permitted.
from-vlan <VLAN-ID>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a single VLAN or a range of VLANs as the match criteria. TCP/UDP packets received from the VLANs identified here are permitted. • <VLAN-ID> – Specify the VLAN ID. To configure a range of VLANs, enter the start and end VLAN IDs separated by a hyphen (for example, 12-20). **Note:** Use this option with WLANs and port ACLs.
host <SOURCE-HOST-IP>	Identifies a specific host (as the source to match) by its IP address. TCP/UDP packets received from the specified host are permitted. • <SOURCE-HOST-IP> – Specify the source host's exact IP address in the A.B.C.D format.
<DEST-IP/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Sets the destination IP address and mask (A.B.C.D/M) to match. TCP/UDP packets addressed to the specified destinations are permitted.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IP address. TCP/UDP packets received from any destination are permitted.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IP address. TCP/UDP packets addressed to the specified host are permitted. • <DEST-HOST-IP> – Specify the destination host's exact IP address in the A.B.C.D format.
<NETWORK-GROUP-ALIAS-NAME>	This keyword is common to the 'tcp' and 'udp' parameters. Applies a network-group alias to identify the destination IP addresses. TCP/UDP packets destined to the addresses identified in the network-group alias are permitted. • <NETWORK-ALIAS-GROUP-NAME> – Specify the network-group alias name (should be existing and configured).
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
eq [<1-65535>| <SERVICE-NAME>| |bgp|dns|ftp| ftp-data|gropher| https|ldap|nntp|ntp| pop3|sip|smtp| ssh|telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated *Border Gateway Protocol* (BGP) protocol port (179) • dns – The designated *Domain Name System* (DNS) protocol port (53) • ftp – The designated *File Transfer Protocol* (FTP) protocol port (21) Contd..

	• ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated *Lightweight Directory Access Protocol* (LDAP) protocol port (389) • nntp – The designated *Network News Transfer Protocol* (NNTP) protocol port (119) • ntp – The designated *Network Time Protocol* (NTP) protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated *Session Initiation Protocol* (SIP) protocol port (5060) • smtp – The designated *Simple Mail Transfer Protocol* (SMTP) protocol port (25) • ssh – The designated *Secure Shell* (SSH) protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated *Trivial File Transfer Protocol* (TFTP) protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all permit events matching this entry. If a source and/or destination IP address or port is matched (i.e. a TCP/UDP packet is received from a specified IP address and/or is destined for a specified IP address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list. The following protocols are supported:

- IP
- ICMP
- ICP
- UDP
- PROTO (any Internet protocol other than TCP, UDP, and ICMP)

The last ACE in the access list is an implicit deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. The packet is allowed or denied based on the ACL configuration.

- Filtering on TCP or UDP allows you to specify port numbers as filtering criteria.
- Select ICMP to allow/deny packets. Selecting ICMP filters ICMP packets based on ICMP type and code.

NOTE: The log option is functional only for router ACL's. The log option displays an informational logging message about the packet matching the entry sent to the console.

Example

```
rfs6000-37FABE(config-ip-acl-test)#show context
ip access-list test
rfs6000-37FABE(config-ip-acl-test)#

rfs6000-37FABE(config-ip-acl-test)#permit ip 172.16.10.0/24 any log rule-
precedence 750
rfs6000-37FABE(config-ip-acl-test)#permit tcp 172.16.10.0/24 any log rule-
precedence 800

rfs6000-37FABE(config-ip-acl-test)#show context
ip access-list test
 permit ip 172.16.10.0/24 any log rule-precedence 750
 permit tcp 172.16.10.0/24 any log rule-precedence 800
rfs6000-37FABE(config-ip-acl-test)#
```

Related Commands

no	Removes a specified IP permit access rule
alias	Creates and configures aliases (network, VLAN, and service)

11.2 mac-access-list

ACCESS-LIST

The following table summarizes MAC Access list configuration commands:

Table 11.2 *MAC-Access-List-Config Commands*

Command	Description	Reference
deny	Creates a new deny access rule or modifies an existing rule. A deny access rule marks packets for rejection.	*page 11-35*
disable	Disables a MAC deny or permit rule without removing it from the ACL	*page 11-38*
ex3500	Creates a MAC ACL deny and/or permit rule applicable only to the EX3500 switch	*page 11-40*
insert	Inserts a rule in an MAC ACL without overwriting or replacing an exciting rule having the same precedence	*page 11-43*
no	Removes a deny and/or a permit access rule from a MAC ACL	*page 11-45*
permit	Creates a new permit access rule or modifies an existing rule. A deny access rule marks packets for forwarding.	*page 11-46*

11.2.1 deny

mac-access-list

Creates a deny rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for rejection. You can also use this command to modify an existing deny rule.

NOTE: Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DEST-MAC>
<DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|
aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence
<1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• deny [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DEST-MAC>
<DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,type [8021q|<1-65535>|
aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-4095>,log,rule-precedence
<1-5000>) {(rule-description <LINE>)}
```

<SOURCE-MAC> <SOURCE-MAC-MASK>	Configures the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask. Packets received from the specified MAC addresses are dropped.
any	Identifies all devices as the source to deny access. Packets received from any source are dropped.
host <SOURCE-HOST-MAC>	Identifies a specific host as the source to deny access • <SOURCE-HOST-MAC> – Specify the source host's exact MAC address to match. Packets received from the specified host are dropped.
<DEST-MAC> <DEST-MAC-MASK>	Configures the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address to match. • <DEST-MAC-MASK> – Specify the destination MAC address mask to match. Packets addressed to the specified MAC addresses are dropped.
any	Identifies all devices as the destination to deny access. Packets addressed to any destination are dropped.
host <DEST-HOST-MAC>	Identifies a specific host as the destination to deny access • <DEST-HOST-MAC> – Specify the destination host's exact MAC address to match. Packets addressed to the specified host are dropped.

dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint | rarp|wisp]	Configures the EtherType value An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk *Address Resolution Protocol* (ARP) payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800) • ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse *Address Resolution Protocol* (ARP) payload (0x8035) • wisp – Indicates the *Wireless Internet Service Provider* (WISP) payload (0x8783)
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1 - 4095.
log	Logs all deny events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is received from a specified MAC address or is destined for a specified MAC address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) data. The MAC access list denies traffic from a particular source MAC address or any MAC address. It can also disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can disallow traffic based on the VLAN and EtherType.

- ARP
- WISP
- IP
- 802.1q

NOTE: MAC ACLs always take precedence over IP based ACLs.

The last ACE in the access list is an implicit deny statement. Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed or denied based on the ACL's configuration.

Example

```
rfs4000-229D58(config-mac-acl-test)#deny 41-85-45-89-66-77 ff-ff-ff-00-00-00 any
 vlan 1 rule-precedence 1

rfs4000-229D58(config-mac-acl-test)#deny host 00-01-ae-00-22-11 any rule-
precedence 2

rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
rfs6000-37FABE(config-mac-acl-test)#deny any host 00:01:ae:00:22:11
```

The following example denies traffic between two hosts based on MAC addresses:

```
rfs6000-37FABE(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
```

Related Commands

no	Removes a specified MAC deny access rule

11.2.2 disable

mac-access-list

Disables a MAC deny or permit rule without removing it from the ACL. A disabled rule is inactive and is not used to filter packets.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
disable [deny|insert|permit]

disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark [8021p <0-
7>|dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|
wisp],vlan <1-4095>) log (rule-precedence <1-5000>) {(rule-description <LINE>)}

disable insert [deny|permit]
```

Parameters

```
• disable [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-
MAC>] [<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark
[8021p <0-7>|dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|
mint|rarp|wisp],vlan <1-4095>) log (rule-precedence <1-5000>) {(rule-description
<LINE>)}
```

disable [deny|insert|permit]	Disables a deny, insert or permit access rule without removing it from the MAC ACL **Note:** Provide the exact values used to configure the deny or permit rule that is to be disabled.
<SOURCE-MAC> <SOURCE-MAC-MASK>	Specifies the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask.
any	Select 'any' if the rule is applicable to any source MAC address
host <SOURCE-HOST-MAC>	Specify the source host's exact MAC address
<DEST-MAC> <DEST-MAC-MASK>	Specifies the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address. • <DEST-MAC-MASK> – Specify the destination MAC address mask.
any	Select 'any' if the rule is applicable to any destination MAC address
host <DEST-HOST-MAC>	Specify the destination host's exact MAC address
log	The following keyword defines the action taken when a packet matches any or all of the above specified criteria • log – Logs a record. when a packet matches the specified criteria

dotp1p <0-7>	Specify the 802.1p priority from 0 - 7.
mark [8021p <0-7>| dscp <0-63>]	Marks/modifies packets that match the criteria specified here • 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 • dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63 **Note:** This option is applicable only to the *disable > permit* MAC ACL rule.
type [8021q| <1-65535>|aarp| appletalk|arp|ip| ipv6|ipx|mint|rarp| wisp]	Use the available options to specify the EtherType value.
vlan <1-4095>	Specify the VLAN ID(s)
log	Select log, if the rule has been configured to log records in case of a match.
rule-precedence <1-5000> {(rule-description <LINE>)}	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Provide the precedence assigned to this deny or permit rule. • <1-5000> – Specify a value from 1 - 5000. The rule with the specified precedence is removed form the MAC ACL. • rule-description <LINE> – Optional. Enter the description configured for this deny or permit rule.

Example

The following example shows the MAC access list 'test' settings before the 'disable' command is executed:

```
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#

rfs4000-229D58(config-mac-acl-test)#disable deny host 00-01-AE-00-22-11 any rule-
precedence 2
```

The following example shows the MAC access list 'test' settings after the 'disable' command is executed:

```
rfs4000-229D58(config-mac-acl-test)#show context
mac access-list test
 deny 41-85-45-89-66-77 FF-FF-FF-00-00-00 any vlan 1 rule-precedence 1
 disable deny host 00-01-AE-00-22-11 any rule-precedence 2
rfs4000-229D58(config-mac-acl-test)#
```

Related Commands

no	Enables a disabled deny or permit rule
deny	Creates a new deny access rule or modifies an existing rule
permit	Creates a new permit access rule or modifies an existing rule

11.2.3 ex3500

mac-access-list

Creates a MAC ACL deny and/or permit rule, applicable only to the EX3500 switch

Each deny or permit rule consists of a set of match criteria and an associated action, which is deny access for the deny rule and allow access for the permit rule. When applied to layer 2 traffic (between a EX3500 switch and the WiNG managed service platform or a WiNG VM interface) every packet is matched against the configured match criteria and in case of a match the packet is dropped or forwarded depending on the rule type.

EX3500 devices (EX3524 and EX3548) are layer 2 Gigabit Ethernet switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. An EX3500 switch has an SNMP-based management agent that provides both in-band and out-of-band management access. The EX3500 switch utilizes an embedded HTTP Web agent and *command line interface* (CLI), which in spite of being different from that of the WiNG operating system provides WiNG controllers PoE and port management resources.

NOTE: To implement the EX3500 MAC ACL rule, apply the MAC ACL directly to a EX3500 device, or to an EX35XX profile. For more information, see *access-group*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2]

ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2] [any |host <SOURCE-MAC>|
network <SOURCE-MAC> <SOURCE-MAC-MASK>] [any|host <DEST-MAC>|network <DEST-MAC>
<DEST-MAC-MASK>] [ethertype <0-65535|ethertype-mask <0-65535>|ex3500-time-range
<TIME-RANGE-NAME>|rule-precedence <1-128>|vlan <1-4094>|vlan-mask <1-4095>]
```

Parameters

```
• ex3500 [deny|permit] [all|tagged-eth2|untagged-eth2] [any|host <SOURCE-MAC>|
network <SOURCE-MAC> <SOURCE-MAC-MASK>] [any|host <DEST-MAC>|network <DEST-MAC>
<DEST-MAC-MASK>] [ethertype <0-65535|ethertype-mask <0-65535>|ex3500-time-range
<TIME-RANGE-NAME>|rule-precedence <1-128>|vlan <1-4094>|vlan-mask <1-4095>]
```

[deny|permit]	Creates a deny or permit MAC ACL rule and configures the rule parameters Every EX3500 MAC ACL rule provides a set of match criteria against which incoming and outgoing packets (to and from an EX3500 device) are matched. In case of a match, the packet is dropped or forwarded depending on the rule type. The packet is dropped in case of a *deny* rule, and forwarded for an *permit* rule.

[all|tagged-eth2| untagged-eth2]	Specifies the packet type • all – Applies this deny/permit rule to all packets • tagged-eth2 – Applies this deny/permit rule only to tagged Ethernet-2 packets • untagged-eth2 – Applies this deny/permit rule only to untagged Ethernet-2 packets After specifying the packet type, configure the source and/or EX3500 MAC addresses to match.

[any| host <SOURCE-MAC>| network <SOURCE-MAC> <SOURCE-MAC-MASK>]	Enter the *Source* MAC addresses
	• any – Identifies all EX3500 devices as a source to match
	• host <SOURCE-MAC> – Identifies a specific EX3500 host as the source to match
	  • <SOURCE-MAC> – Specify the source host's exact MAC address
	• network <SOURCE-MAC> <SOURCE-MAC-MASK> – Configures a range of MAC addresses as the source to match. Packets received from any of these MAC addresses are dropped.
	  • <SOURCE-MAC> – Specify the source MAC address to match.
	  • <SOURCE-MAC-MASK> – Specify the source MAC bit mask.
	For a deny rule, packets received from EX3500 device(s) matching the specified MAC address(es) are dropped.
	For a permit rule, packets received from EX3500 device(s) matching the specified MAC address(es) are forwarded.

[any|host <DEST-MAC>| network <DEST-MAC> <DEST-MAC-MASK>]	Enter the *Destination* MAC addresses
	• any – Identifies all EX3500 devices as a destination to match
	• host <SOURCE-MAC> – Identifies a specific EX3500 host as the destination to match
	  • <SOURCE-MAC> – Specify the destination host's exact MAC address
	• network <SOURCE-MAC> <SOURCE-MAC-MASK> – Configures a range of MAC addresses as the destination to match. Packets addressed to any of these MAC addresses are dropped.
	  • <SOURCE-MAC> – Specify the destination MAC address to match.
	  • <SOURCE-MAC-MASK> – Specify the destination MAC bit mask.
	For a deny rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are dropped.
	For a permit rule, packets addressed to EX3500 device(s) matching the specified MAC address(es) are forwarded.

ether-type <0-65535>	Configures the Ethertype protocol number. The ether type is a two-octet field within an Ethernet frame. It indicates the protocol encapsulated in the payload of an Ethernet frame. • <0-65535> – Specify the value from 0 - 65535. The default value is 1.
ethertype-mask <0-65535>	Configures the Ethertype mask • <0-65535> – Specify the value from 0 - 65535. The default value is 1.

ex3500-time-range <TIME-RANGE-NAME>	Applies a specified EX3500 time range (should be existing and configured). The deny or permit rule is applied during the time period specified in the EX3500 time range. • <TIME-RANGE-NAME> – Specify the time range name. An EX3500 time range list consists of a set of periodic and absolute time range rules. Periodic time ranges recur periodically at specified time periods, such as daily, weekly, weekends, weekdays, and on specific week days, for example on every successive Mondays. Absolute time ranges are not periodic and do not recur. They consist of a range of days during a particular time period (the starting and ending days and time are fixed). **Note:** For information on configuring EX3500 time-range, see *ex3500*.
vlan <1-4094>	Configures a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server) • <1-4094> – Specify the VLAN ID from 1 - 4094.
vlan-mask <1-4095>	Configures the VLAN ID bit mask value • <1-4095> – Specify the VLAN bit mask from 1 - 4095.
rule-precedence <1-128>	Configures a precedence for this EX3500 MAC ACL • <1 - 128> – Specify a value from 1 - 128. ACLs with lower precedence are applied first to packets.

Example

```
nx9500-6C8809(config-mac-acl-ex3500MacACL)#ex3500 deny tagged-eth2 any any vlan
20 rule-precedence 1

nx9500-6C8809(config-mac-acl-ex3500MacACL)#show context
mac access-list ex3500MacACL
 ex3500 deny tagged-eth2 any any vlan 20 rule-precedence 1
nx9500-6C8809(config-mac-acl-ex3500MacACL)#
```

11.2.4 insert

mac-access-list

Enables the insertion of a rule in an MAC ACL without overwriting or replacing an existing rule having the same precedence

The insert option allows a new rule to be inserted within a MAC ACL. Consider an MAC ACL consisting of rules having precedences 1, 2, 3, 4, 5, and 6. You want to insert a new rule with precedence 4, without overwriting the existing precedence 4 rule. Using the insert option inserts the new rule prior to the existing one. The existing precedence 4 rule's precedence changes to 5, and the change cascades down the list of rules within the ACL. That means rule 5 becomes rule 6, and rule 6 becomes rule 7.

NOTE: NOT using insert when creating a new rule having the same precedence as an existing rule, overwrites the existing rule.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
insert [deny|permit] <PARAMETERS> (dot1p <0-7>,mark [8021p <0-7>|dscp <0-63>],
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-
4095>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• insert [deny|permit] <PARAMETERS> (dot1p <0-7>,mark [8021p <0-7>|dscp <0-63>],
type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan <1-
4095>,log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

insert [deny|permit]	Inserts a deny or permit rule within an MAC ACL
<PARAMETERS>	Provide the match criteria for this deny/permit rule. Packets will be filtered based on the criteria set here. For more information on the deny rule, see *deny*. For more information on the permit rule, see *permit*.
dot1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
mark [8021p <0-7>| dscp <0-63>]	Marks/modifies packets that match the criteria specified here • 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 • dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63 **Note:** This option is applicable only to the *insert > permit* MAC ACL rule.

type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint| rarp|wisp]	Configures the EtherType value An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk ARP payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the IPv4 payload (0x0800) • ipv6 – Indicates the IPv6 payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse ARP payload (0x8035) • wisp – Indicates the WISP payload (0x8783)
vlan <1-4095>	Configures the VLAN where the traffic is received • <1-4095> – Specify the VLAN ID from 1 - 4095.
log	Logs all deny/permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is received from a specified MAC address or is destined for a specified MAC address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Example

```
rfs4000-229D58(config-mac-acl-test1)#deny 11-22-33-44-55-66 11-22-33-44-55-77 any
rule-precedence 1
rfs4000-229D58(config-mac-acl-test1)#deny host B4-C7-99-6D-CD-9B any rule-
precedence 2

rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
 deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
 deny host B4-C7-99-6D-CD-9B any rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#

In the following example a new rule is inserted between the rules having precedences
1 and 2. The precedence of the existing precedence '2' rule changes to precedence 3.

rfs4000-229D58(config-mac-acl-test1)#insert permit host B4-C7-99-6D-B5-D6 host B4-
C7-99-6D-CD-9B rule-precedence 2
rfs4000-229D58(config-mac-acl-test1)#show context
mac access-list test1
 deny 11-22-33-44-55-66 11-22-33-44-55-77 any rule-precedence 1
 permit host B4-C7-99-6D-B5-D6 host B4-C7-99-6D-CD-9B rule-precedence 2
 deny host B4-C7-99-6D-CD-9B any rule-precedence 3
rfs4000-229D58(config-mac-acl-test1)#
```

11.2.5 no

mac-access-list

Negates a command or sets its default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [deny|disable|permit]

no [deny|permit] [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>]
[<DEST-MAC> <DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark [8021p <0-
7>|dscp <0-63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|
wisp],vlan <1-4095>) log (rule-precedence <1-5000>) {(rule-description <LINE>)}

no disable [deny|permit] <RULE-PARAMETERS>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny or permit rule from the MAC ACL

Example

```
rfs6000-37FABE(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence
610
deny any host 33-44-55-66-77-88 log rule-precedence 700

rfs6000-37FABE(config-mac-acl-test)#no deny any host 33-44-55-66-77-88 log
rule-precedence 700

rfs6000-37FABE(config-mac-acl-test)#show context
mac access-list test
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence
610
```

11.2.6 permit

mac-access-list

Creates a permit rule that marks packets (from a specified source MAC and/or to a specified destination MAC) for forwarding. You can also use this command to modify an existing permit rule.

NOTE: Use a decimal value representation to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed EtherType. Use the decimal equivalent of the EtherType listed for any other EtherType.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DEST-MAC>
<DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark [8021p <0-7>,dscp <0-
63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan
<1-4095>) log (rule-precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• permit [<SOURCE-MAC> <SOURCE-MAC-MASK>|any|host <SOURCE-HOST-MAC>] [<DEST-MAC>
<DEST-MAC-MASK>|any|host <DEST-HOST-MAC>] (dot1p <0-7>,mark [8021p <0-7>,dscp <0-
63>],type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp],vlan
<1-4095>) log (rule-precedence <1-5000>) {(rule-description <LINE>)}
```

<SOURCE-MAC> <SOURCE-MAC-MASK>	Configures the source MAC address and mask to match • <SOURCE-MAC> – Specify the source MAC address to match. • <SOURCE-MAC-MASK> – Specify the source MAC address mask. Packets addressed to the specified MAC addresses are forwarded.
any	Identifies all devices as the source to permit access. Packets addressed from any source are forwarded.
host <SOURCE-HOST-MAC>	Identifies a specific host as the source to permit access • <SOURCE-HOST-MAC> – Specify the source host's exact MAC address to match. Packets addressed to the specified host are forwarded.
<DEST-MAC> <DEST-MAC-MASK>	Configures the destination MAC address and mask to match • <DEST-MAC> – Specify the destination MAC address to match. • <DEST-MAC-MASK> – Specify the destination MAC address mask to match. Packets addressed to the specified MAC addresses are forwarded.
DEST-MAC-MASK	Specifies the destination MAC address mask to match
any	Identifies all devices as the destination to permit access. Packets addressed to any destination are forwarded.

host <DEST-HOST-MAC>	Identifies a specific host as the destination to permit access • <DEST-HOST-MAC> – Specify the destination host's exact MAC address to match. Packets addressed to the specified host are forwarded.
dotp1p <0-7>	Configures the 802.1p priority value. Sets the service classes for traffic handling • <0-7> – Specify 802.1p priority from 0 - 7.
mark [8021p <0-7>, dscp <0-63>]	Marks/modifies packets that match the criteria specified here • 8021p <0-7> – Modifies 802.1p VLAN user priority from 0 - 7 • dscp <0-63> – Modifies DSCP TOS bits in the IP header from 0 - 63 **Note:** This option is applicable only to the MAC ACL permit rule.
type [8021q|<1-65535>| aarp|appletalk| arp|ip|ipv6|ipx|mint | rarp|wisp]	Configures the EtherType value An EtherType is a two-octet field in an Ethernet frame that indicates the protocol encapsulated in the payload of the frame. The EtherType values are: • 8021q – Indicates a 802.1q payload (0x8100) • <1-65535> – Indicates the EtherType protocol number • aarp – Indicates the Appletalk *Address Resolution Protocol* (ARP) payload (0x80F3) • appletalk – Indicates the Appletalk Protocol payload (0x809B) • arp – Indicates the ARP payload (0x0806) • ip – Indicates the Internet Protocol, Version 4 (IPv4) payload (0x0800) • ipv6 – Indicates the Internet Protocol, Version 6 (IPv6) payload (0x86DD) • ipx – Indicates the Novell's IPX payload (0x8137) • mint – Indicates the MiNT protocol payload (0x8783) • rarp – Indicates the reverse *Address Resolution Protocol* (ARP) payload (0x8035) • wisp – Indicates the *Wireless Internet Service Provider* (WISP) payload (0x8783)
vlan <1-4095>	Configures the VLAN ID • <1-4095> – Specify the VLAN ID from 1 - 4095.
log	Logs all permit events matching this entry. If a source and/or destination MAC address is matched (i.e. a packet is addressed to a specified MAC address or is destined for a specified MAC address), an event is logged.
rule-precedence <1-5000> rule-description <LINE>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10. • rule-description – Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Usage Guidelines

The permit command in the MAC ACL allows traffic based on layer 2 (data-link layer) information. A MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, or Ethernet type. Common types include:

- ARP
- WISP
- IP
- 802.1q

Layer 2 traffic is not allowed by default. To adopt an access point through an interface, configure an ACL to allow an Ethernet WISP.

Use the mark option to specify the type of service (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is marked based on the ACL's configuration.

NOTE: To apply an IP based ACL to an interface, a MAC access list entry is mandatory to allow ARP. A MAC ACL always takes precedence over IP based ACLs.

Example

```
rfs6000-37FABE(config-mac-acl-test)#permit host 11-22-33-44-55-66 any log mark
8021p 3 rule-precedence 600

rfs6000-37FABE(config-mac-acl-test)#permit host 22-33-44-55-66-77 host 11-22-33-
44-55-66 type ip log rule-precedence 610

rfs6000-37FABE(config-mac-acl-test)#show context
mac access-list testPF
 permit host 11-22-33-44-55-66 any log mark 8021p 3 rule-precedence 600
 permit host 22-33-44-55-66-77 host 11-22-33-44-55-66 type ip log rule-precedence
610
rfs6000-37FABE(config-mac-acl-test)#
```

Related Commands

no	Removes or resets a specified MAC ACL permit rule

11.3 ipv6-access-list

ACCESS-LIST

Configures a IPv6 ACL

An IPv6 ACL defines a set of rules that filter IPv6 packets flowing through a port or interface. Each rule specifies the action taken when a packet matches the rule. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed.

The WiNG software supports IPv6 only on VLAN interfaces. Therefore, IPv6 ACLs can be applied only on the VLAN interface.

The following table summarizes IPv6 access list configuration commands:

Table 11.3 *IPv6-Access-List-Config Commands*

Command	Description	Reference
deny	Creates a deny access rule or modifies an existing rule. A deny access rule rejects IPv6 packets from specified address(es) and/or destined for specified address(es).	*page 11-50*
no	Removes a deny and/or a access rule from a IPv6 ACL	*page 11-56*
permit	Creates a permit access rule or modifies an existing rule. A permit access rule accepts IPv6 packets from specified address(es) and/or destined for specified address(es).	*page 11-57*

11.3.1 deny

ipv6-access-list

Creates a deny rule that rejects packets from a specified IPv6 source and/or to a specified IPv6 destination. You can also use this command to modify an existing deny rule.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
deny [icmpv6|ipv6|proto|tcp|udp]

deny icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|
any|host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-CODE>
<ENDING-ICMPv6-CODE>]|type [eq <ICMPV6-TYPE>|range <STARTING-ICMPv6-TYPE>
<ENDING-ICMPv6-TYPE>]] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

deny ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-
description <LINE>)}

deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

deny [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>]
[eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|
pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-
precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• deny icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-
CODE> <ENDING-ICMPv6-CODE>]|type [eq <ICMPV6-TYPE>|range <STARTING-ICMPv6-TYPE>
<ENDING-ICMPv6-TYPE>]] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

icmpv6	Applies this deny rule to ICMPv6 packets only
<SOURCE-IPv6/MASK>	Specifies a range of IPv6 source address (network) to match. ICMPv6 packets received from any source in the specified network are dropped.
any	Specifies the source as any IPv6 address. ICMPv6 packets received from any source are dropped.
host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. ICMPv6 packets received from the specified host are dropped. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	Specifies a range of IPv6 destination address (network) to match. ICMPv6 packets addressed to any destination within the specified network are dropped.
any	Specifies the destination as any IPv6 address. ICMPv6 packets addressed to any destination are dropped.

host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. ICMPv6 packets addressed to the specified host are dropped. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
<ICMPv6-TYPE> [eq|range]	Defines the ICMPv6 type field filter • eq – Configures a specific ICMPv6 type. Specify the ICMPv6 type value. • range – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values. **Note:** ICMPv6 packets with type field value matching the values specified here are dropped.
<ICMPv6-CODE>	Defines the ICMPv6 code field filter • eq – Configures a specific ICMPv6 code. Specify the ICMPv6 code value. • range – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values. **Note:** ICMPv6 packets with code field value matching the values specified here are dropped.
log	Logs all deny events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

• `deny ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}`

ipv6	Applies this deny rule to IPv6 packets only
<SOURCE-IPv6/MASK>	Specifies a range of IPv6 source address (network) to match. IPv6 packets received from any source in the specified network are dropped.
any	Specifies the source as any IPv6 address. IPv6 packets received from any source are dropped.
host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. IPv6 packets received from the specified host are dropped. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	Specifies a range of IPv6 destination address (network) to match. IPv6 packets addressed to any destination within the specified network are dropped.
any	Specifies the destination as any IPv6 address. IPv6 packets addressed to any destination are dropped.
host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. IPv6 packets addressed to the specified host are dropped. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.

log	Logs all deny events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000 **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• deny proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

proto	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.
<PROTOCOL-NUMBER>	Filters protocols using their *Internet Assigned Numbers Authority* (IANA) protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.
gre	Identifies the GRE protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.
igp	Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF.
ospf	Identifies the OSPF protocol (number 89) OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

vrrp	Identifies the VRRP protocol (number 112) VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
<SOURCE-IPv6/MASK>	Specifies a range of IPv6 source address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source in the specified network are dropped.
any	Specifies the source as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are dropped.
host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	Specifies a range of IPv6 destination address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination within the specified network are dropped.
any	Specifies the destination as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are dropped.
host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified host are dropped. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
log	Logs all deny events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

• `deny [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>] [eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-precedence <1-5000>)` *`{(rule-description <LINE>)}`*

tcp	Applies this deny rule to TCP packets only
udp	Applies this deny rule to UDP packets only
<SOURCE-IPv6/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 source address (network) to match. TCP/UDP packets received from any source in the specified network are dropped.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IPv6 address. TCP/UDP packets received from any source are dropped.

host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. TCP/UDP packets received from the specified host are dropped. • <SOURCE-HOST-IP> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 destination address (network) to match. TCP/UDP packets addressed to any destination within the specified network are dropped.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IPv6 address. TCP/UDP packets received from any destination are dropped.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
host <DEST-HOST-IP>	Identifies a specific host (as the destination to match) by its IPv6 address. TCP/UDP packets addressed to the specified host are dropped. • <DEST-HOST-IP> – Specify the destination host's exact IP address.
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
eq [<1-65535>| <SERVICE-NAME>| |bgp|dns|ftp| ftp-data|gropher| https|ldap|nntp|ntp| pop3|sip|smtp| ssh|telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated BGP protocol port (179) • dns – The designated DNS protocol port (53) • ftp – The designated FTP protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated LDAP protocol port (389) • nntp – The designated NNTP protocol port (119) • ntp – The designated NTP protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated SIP protocol port (5060) • smtp – The designated SMTP protocol port (25) • ssh – The designated SSH protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated TFTP protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all deny events matching this entry

rule-precedence <1-5000>	Assigns a precedence for this deny rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this deny rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Example

```
rfs6000-81742D(config-ipv6-acl-test)#deny icmpv6 any any type eq 1 code eq 0 log
rule-precedence 1

rfs6000-81742D(config-ipv6-acl-test)#show context
ipv6 access-list test
 deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-
command log rule-precedence 1
rfs6000-81742D(config-ipv6-acl-test)#
```

Related Commands

no	Removes a specified deny access rule

11.3.2 no

ipv6-access-list

Removes a deny or permit rule

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [deny|permit]

no [deny|permit] [icmpv6|ipv6|proto|tcp|udp] <RULE-PARAMETERS> {(rule-description <LINE>)}
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny or permit rule from the selected IPv6 access list

Example

The following example shows the ACL 'test' settings before the 'no' commands are executed:

```
rfs6000-81742D(config-ipv6-acl-test)#show context
ipv6 access-list test
 deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-
command log rule-precedence 1
 permit proto gre any any log rule-precedence 2
rfs6000-81742D(config-ipv6-acl-test)#

rfs6000-81742D(config-ipv6-acl-test)#no deny icmpv6 any any type eq 1 log
rule-precedence 1

rfs6000-81742D(config-ipv6-acl-test)#show context
ipv6 access-list test
 permit proto gre any any log rule-precedence 2
rfs6000-81742D(config-ipv6-acl-test)#
```

11.3.3 permit

ipv6-access-list

Creates a permit rule that accepts packets from a specified IPv6 source and/or to a specified IPv6 destination. You can also use this command to modify an existing permit rule.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
permit [icmpv6|ipv6|proto|tcp|udp]

permit icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-
CODE> <ENDING-ICMPv6-CODE>]|type [eq <ICMPV6-TYPE>|range <STARTING-ICMPv6-TYPE>
<ENDING-ICMPv6-TYPE>]] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

permit ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-
description <LINE>)}

permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host
<DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}

permit [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>]
[eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|ntp|
pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-
precedence <1-5000>) {(rule-description <LINE>)}
```

Parameters

```
• permit icmpv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|host <DEST-HOST-IPv6>] [code [eq <ICMPv6-CODE>|range <STARTING-ICMPv6-
CODE> <ENDING-ICMPv6-CODE>]|type [eq <ICMPV6-TYPE>|range <STARTING-ICMPv6-TYPE>
<ENDING-ICMPv6-TYPE>]] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

icmpv6	Applies this permit rule to ICMPv6 packets only
<SOURCE-IPv6/MASK>	Specifies a range of IPv6 source address (network) to match. ICMPv6 packets received from any source in the specified network are accepted.
any	Specifies the source as any IPv6 address. ICMPv6 packets received from any source are accepted.
host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. ICMPv6 packets received from the specified host are accepted. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	Specifies a range of IPv6 destination address (network) to match. ICMPv6 packets addressed to any destination within the specified network are accepted.
any	Specifies the destination as any IPv6 address. ICMPv6 packets addressed to any destination are accepted.

host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. ICMPv6 packets addressed to the specified host are accepted. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
<ICMPv6-TYPE> [eq|range]	Defines the ICMPv6 type field filter • eq – Configures a specific ICMPv6 type. Specify the ICMPv6 type value. • range – Configures a range of ICMPv6 types. Specify the starting and ending ICMPv6 type values. **Note:** ICMPv6 packets with type field value matching the values specified here are forwarded.
<ICMPv6-CODE>	Defines the ICMPv6 code field filter • eq – Configures a specific ICMPv6 code. Specify the ICMPv6 code value. • range – Configures a range of ICMPv6 code. Specify the starting and ending ICMPv6 code values. **Note:** ICMPv6 packets with code field value matching the values specified here are forwarded.
log	Logs all permit events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

• `permit ipv6 [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>)` *`{(rule-description <LINE>)}`*

ipv6	Applies this permit rule to IPv6 packets only
<SOURCE-IPv6/MASK>	Specifies a range of IPv6 source address (network) to match. IPv6 packets received from any source in the specified network are forwarded.
any	Specifies the source as any IPv6 address. IPv6 packets received from any source are forwarded.
host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. IPv6 packets received from the specified host are forwarded. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	Specifies a range of IPv6 destination address (network) to match. IPv6 packets addressed to any destination within the specified network are forwarded.
any	Specifies the destination as any IPv6 address. IPv6 packets addressed to any destination are forwarded.
host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. IPv6 packets addressed to the specified host are forwarded. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.

log	Logs all permit events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000 **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• permit proto [<PROTOCOL-NUMBER>|<PROTOCOL-NAME>|eigrp|gre|igp|ospf|vrrp]
[<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/MASK>|any|
host <DEST-HOST-IPv6>] (log,rule-precedence <1-5000>) {(rule-description <LINE>)}
```

proto	Configures the ACL for additional protocols Additional protocols (other than IP, ICMP, TCP, and UDP) must be configured using this parameter.
<PROTOCOL-NUMBER>	Filters protocols using their *Internet Assigned Numbers Authority* (IANA) protocol number • <PROTOCOL-NUMBER> – Specify the protocol number.
<PROTOCOL-NAME>	Filters protocols using their IANA protocol name • <PROTOCOL-NAME> – Specify the protocol name.
eigrp	Identifies the EIGRP protocol (number 88) EIGRP enables routers to maintain copies of neighbors' routing tables. Routers use this information to determine the fastest route to a destination. When a router fails to find a route in its stored route tables, it sends a query to neighbors who in turn query their neighbors till a route is found. EIGRP also enables routers to inform neighbors of changes in their routing tables.
gre	Identifies the GRE protocol (number 47) GRE is a tunneling protocol that enables transportation of protocols (IP, IPX, DEC net, etc.) over an IP network. GRE encapsulates the packet at the source and removes the encapsulation at the destination.
igp	Identifies any private internal gateway (primarily used by CISCO for their IGRP) (number 9) IGP enables exchange of information between hosts and routers within a managed network. The most commonly used IGP protocols are: RIP and OSPF.
ospf	Identifies the OSPF protocol (number 89) OSPF is a link-state IGP. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

vrrp	Identifies the VRRP protocol (number 112) VRRP allows a pool of routers to be advertized as a single virtual router. This virtual router is configured by hosts as their default gateway. VRRP elects a master router, from this pool, and assigns it a virtual IP address. The master router routes and forwards packets to hosts on the same subnet. When the master router fails, one of the backup routers is elected as the master and its IP address is mapped to the virtual IP address.
<SOURCE-IPv6/MASK>	Specifies a range of IPv6 source address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source in the specified network are forwarded.
any	Specifies the source as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from any source are forwarded.
host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) received from the specified host are forwarded. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	Specifies a range of IPv6 destination address (network) to match. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination within the specified network are forwarded.
any	Specifies the destination as any IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to any destination are forwarded.
host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. Packets (EIGRP, GRE, IGMP, IGP, OSPF, or VRRP) addressed to the specified host are forwarded. • <DEST-HOST-IPv6> – Specify the destination host's exact IPv6 address.
log	Logs all permit events matching this entry
rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

```
• permit [tcp|udp] [<SOURCE-IPv6/MASK>|any|host <SOURCE-HOST-IPv6>] [<DEST-IPv6/
MASK>|any|eq <SOURCE-PORT>|host <DEST-HOST-IPv6>|range <START-PORT> <END-PORT>]
[eq [<1-65535>|<SERVICE-NAME>|bgp|dns|ftp|ftp-data|gopher|https|ldap|nntp|
ntp|pop3|sip|smtp|ssh|telnet|tftp|www]|range <START-PORT> <END-PORT>] (log,rule-
precedence <1-5000>) {(rule-description <LINE>)}
```

tcp	Applies this permit rule to TCP packets only
udp	Applies this permit rule to UDP packets only
<SOURCE-IPv6/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 source address (network) to match. TCP/UDP packets received from any source in the specified network are forwarded.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the source as any IPv6 address. TCP/UDP packets received from any source are forwarded.

host <SOURCE-HOST-IPv6>	Identifies a specific host (as the source to match) by its IPv6 address. TCP/UDP packets received from the specified host are forwarded. • <SOURCE-HOST-IPv6> – Specify the source host's exact IPv6 address.
<DEST-IPv6/MASK>	This keyword is common to the 'tcp' and 'udp' parameters. Specifies a range of IPv6 destination address (network) to match. TCP/UDP packets addressed to any destination within the specified network are forwarded.
any	This keyword is common to the 'tcp' and 'udp' parameters. Specifies the destination as any destination IPv6 address. TCP/UDP packets received from any destination are forwarded.
eq <SOURCE-PORT>	Identifies a specific source port • <SOURCE-PORT> – Specify the exact source port.
host <DEST-HOST-IPv6>	Identifies a specific host (as the destination to match) by its IPv6 address. TCP/UDP packets addressed to the specified host are forwarded. • <DEST-HOST-IPv6> – Specify the destination host's exact IP address.
range <START-PORT> <END-PORT>	Specifies a range of source ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
eq [<1-65535>| <SERVICE-NAME>| |bgp|dns|ftp| ftp-data|gropher| https|ldap|nntp|ntp| pop3|sip|smtp| ssh|telnet| tftp|www]	Identifies a specific destination or protocol port to match • <1-65535> – The destination port is designated by its number • <SERVICE-NAME> – Specifies the service name • bgp – The designated BGP protocol port (179) • dns – The designated DNS protocol port (53) • ftp – The designated FTP protocol port (21) • ftp-data – The designated FTP data port (20) • gropher – The designated GROPHER protocol port (70) • https – The designated HTTPS protocol port (443) • ldap – The designated LDAP protocol port (389) • nntp – The designated NNTP protocol port (119) • ntp – The designated NTP protocol port (123) • pop3 – The designated POP3 protocol port (110) • sip – The designated SIP protocol port (5060) • smtp – The designated SMTP protocol port (25) • ssh – The designated SSH protocol port (22) • telnet – The designated Telnet protocol port (23) • tftp – The designated TFTP protocol port (69) • www – The designated www protocol port (80)
range <START-PORT> <END-PORT>	Specifies a range of destination ports • <START-PORT> – Specify the first port in the range. • <END-PORT> – Specify the last port in the range.
log	Logs all permit events matching this entry

rule-precedence <1-5000>	Assigns a precedence for this permit rule • <1-5000> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 10.
rule-description <LINE>	Optional. Configures a description for this permit rule. Provide a description that uniquely identifies the purpose of this rule (should not exceed 128 characters in length).

Example

```
rfs6000-81742D(config-ipv6-acl-test)#permit proto gre any any log rule-precedence
2

rfs6000-81742D(config-ipv6-acl-test)#show context
ipv6 access-list test
 deny icmpv6 any any type eq destination-unreachable code eq router-renumbering-
command log rule-precedence 1
 permit proto gre any any log rule-precedence 2
rfs6000-81742D(config-ipv6-acl-test)#
```

Related Commands

no	Removes a specified permit access rule

11.4 ip-snmp-access-list

ACCESS-LIST

SNMP performs network management functions using a data structure called a *Management Information Base* (MIB). SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.

Use SNMP ACLs to help reduce SNMP's vulnerabilities, as SNMP traffic can be exploited to produce a *denial of service* (DoS).

The following table summarizes SNMP access list configuration commands:

Table 11.4 *SNMP-Access-List-Config Commands*

Command	Description	Reference
deny	Creates a deny SNMP MIB object traffic rule	*page 11-64*
permit	Creates a permit SNMP MIB object traffic rule	*page 11-65*
no	Removes a deny or permit SNMP MIB object traffic rule	*page 11-66*

11.4.1 deny

ip-snmp-access-list

Creates a deny SNMP MIB object traffic rule. Use this command to specify the match criteria based on which SNMP traffic is denied

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
deny [<IP/M>|any|host <IP>]
```

Parameters

- `deny [<IP/M>|any|host <IP>]`

deny [<IP/M>| any|host <IP>]	Configures the match criteria for this deny rule • <IP/M> – Specifies a network address and mask in the A.B.C.D/M format. Packets received or destined for this network are dropped • any – Specifies the match criteria as any. Packets received or destined from any address are dropped • host <IP> – Identifies a host by its IP address. Packets received or destined for this host are dropped

Example

```
rfs6000-81742D(config-ip-snmp-acl-test)#deny 192.168.13.0/24

rfs6000-81742D(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 deny 192.168.13.0/24
rfs6000-81742D(config-ip-snmp-acl-test)#
```

Related Commands

no	Removes this deny rule form the IP SNMP ACL

11.4.2 permit

ip-snmp-access-list

Creates a permit SNMP MIB object traffic rule. Use this command to specify the match criteria based on which SNMP traffic is permitted.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
permit [<IP/M>|any|host <IP>]
```

Parameters

- `permit [<IP/M>|any|host <IP>]`

permit [<IP/M>| any|host <IP>]	Configures the match criteria for this permit rule • <IP/M> – Specifies a network address and mask in the A.B.C.D/M format. Packets received or destined for this network are forwarded • any – Specifies the match criteria as any. Packets received or destined from any address are forwarded • host <IP> – Identifies a host by its IP address. Packets received or destined for this host are forwarded

Example

```
rfs6000-81742D(config-ip-snmp-acl-test)#permit host 192.168.13.13

rfs6000-81742D(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 permit host 192.168.13.13
 deny 192.168.13.0/24
rfs6000-81742D(config-ip-snmp-acl-test)#
```

Related Commands

no	Removes this permit rule form the IP SNMP ACL

11.4.3 no

ip-snmp-access-list

Removes a deny or permit rule from the IP SNMP ACL. Use this command to remove IP SNMP ACL as they become obsolete for filtering network access permissions.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [deny|permit] [<IP/M>|any|host <IP>]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes deny and/or permit access rule from this IP SNMP ACL

Example

```
rfs6000-81742D(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 permit host 192.168.13.13
 deny 192.168.13.0/24
rfs6000-81742D(config-ip-snmp-acl-test)#

rfs6000-81742D(config-ip-snmp-acl-test)#no permit host 192.168.13.13

rfs6000-81742D(config-ip-snmp-acl-test)#show context
ip snmp-access-list test
 deny 192.168.13.0/24
rfs6000-81742D(config-ip-snmp-acl-test)#
```

11.5 ex3500-ext-access-list

ACCESS-LIST

IP ACLs function as firewalls that filter or mark packets on layer 3 ports as opposed to MAC ACLs that filter traffic on layer 2 ports.

An IPv4 EX3500 extended ACL is a policy-based ACL that either prevents or allows specific clients from using the EX3500 switch. It allows you to permit or deny client access by specifying that the traffic *from* a specific host or network and/or the traffic *to* a specific host or network be either denied or permitted.

An EX3500 extended ACL consists of a set of deny /permit *rules* that filter packets based on both source and destination IPv4 addresses. Each rule specifies a set of match criteria (the source and destination IP addresses) and has a unique *precedence* value assigned. These ACL rules are applied sequentially to the traffic at a port, by a firewall-supported device, in an increasing order of their precedence. When a packet matches the criteria specified in a rule the packet is either forwarded or dropped based on the rule type.

The following table summarizes IPv4 EX3500 extended ACL configuration commands:

NOTE: To implement the EX3500 extended ACL, apply it directly to a EX3500 device, or to an EX35XX profile. For more information, see *access-group*.

Table 11.5 *EX3500-Extended-Access-List-Config Commands*

Command	Description	Reference
deny	Creates a deny access rule or modifies an existing rule. A deny access rule rejects packets from specified address(es) and/or destined to specified address(es).	*page 11-68*
permit	Creates a permit access rule or modifies an existing rule. A permit access rule accepts packets from specified address(es) and/or destined to specified address(es).	*page 11-71*
no	Removes a deny and/or a permit access rule from this IPv4 EX3500 extended ACL	*page 11-74*

11.5.1 deny

ex3500-ext-access-list

Creates a deny ACL rule that filters packets based on the source and/or destination IPv4 address, and other specified criteria. You can also use this command to modify an existing deny rule.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

```
deny [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|
destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|
ex3500-time-range <TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|
source-port <0-65535>|source-port-bitmark <0-65535>]
```

Parameters

```
• deny [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|
destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|
ex3500-time-range <TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|
source-port <0-65535>|source-port-bitmark <0-65535>]
```

deny [<0-255>| tcp|udp]	Creates a deny rule and identifies the protocol type. This deny rule is applied only to packets matching the protocol specified here. • <0-255> – Identifies the protocol from its number. Specify the protocol number from 0 - 255. • tcp – Configures the protocol as TCP • udp – Configures the protocol as UDP
[<SOURCE-NETWORK-IP/MASK>| any| host <SOURCE-HOST-IP>]	Specifies the source IP address as *any*, *host*, or *network* • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
[<DEST-NETWORK-IP/MASK>| any| host <DEST-HOST-IP>]	Specifies the destination IP address as *any*, *host*, or *network*. • <DEST-NETWORK-IP/MASK> – Configures a network as the destination. Provide the network's IPv4 address along with the mask • host <DEST-HOST-IP> – Configures a single device as the destination. Provide the host device's IPv4 address • any – Specifies that the destination can be any device
control-flag <0-63>	Configures the decimal number (representing a bit string) that specifies the control flag bits in byte 14 of the TCP header <0-63> – Specify a value from 0 - 63. **Note:** Control flags can be used only in ACLs designed to filter TCP traffic. Contd..

	The TCP header contains several one-bit boolean fields known as flags that influence flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags. • URG flag - Marks incoming packet as urgent. • ACK flag - Acknowledges receipt of packet • PUSH flag - Ensures that the packet is given appropriate priority. Often used at the beginning and end of data transfer. • RST flag - Resets the connection. Happens when remote host receives a establish connection packet, but does not have a service waiting to answer and sends a reply with reset flag. • SYN flag - Establishes the 3-way handshake between two hosts • FIN flag - Tears down the connection established between two hosts via the 3-way SYN process
destination-port <0-65535>	Configures the protocol destination port to match. The destination protocol can be TCP, UDP or any other protocol identified by its number (<0-255>). • <0-65535> – Specify the destination port from 0 - 65535.
destination-port-bitmark <0-65535>	Configures the decimal number representing the protocol destination port bits to match • <0-65535> – Specify the destination port bits from 0 - 65535.
dscp <0-63>	Configures the DSCP priority level • <0-63> – Specify a value from 0 - 63. **Note:** If specifying DSCP priority, ip-precedence cannot be specified.
ex3500-time-range <TIME-RANGE-NAME>	Applies a periodic or absolute time range to this rule • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see *ex3500*.
ip-precedence <0-7>	Configures the IP header precedence • <0-7> – Specify a value from 0 - 7.
source-port <0-65535>	Configures the protocol source port to match. The source protocol can be TCP, UDP or any other protocol identified by its number (<0-255>). • <0-65535> – Specify the source port from 0 - 65535.
source-port-bitmark <0-65535>	Configures the decimal number representing the protocol source port bits to match <0-65535> – Specify the source port bits from 0 - 65535.
rule-precedence <1-128>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence to this deny rule • <1-128> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 4 and is applied first to packets.

Usage Guidelines

Use this command to deny traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- TCP
- UDP
- <0-255> (any Internet protocol other than TCP, UDP, and ICMP)

Packet content is checked against the ACEs in the ACL, and are allowed or denied access based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria

Example

The following example denies TCP outgoing packets from all sources p indentwithin the 192.168.14.0 network to a specific host 192.168.13.13:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#deny tcp 192.168.14.0/24 host
192.168.13.13 rule-precedence 1#

nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

Related Commands

no	Removes a specified deny access rule from this IPv4 EX3500 extended ACL

11.5.2 permit

ex3500-ext-access-list

Creates a permit ACL rule that filters packets based on the source and/or destination IPv4 address, and other specified criteria. You can also use this command to modify an existing permit rule.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

```
permit [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NEWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|destination-
port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|ex3500-time-range
<TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|source-port <0-
65535>|source-port-bitmark <0-65535>]
```

Parameters

```
• permit [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>]
[<DEST-NEWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|destination-
port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|ex3500-time-range
<TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|source-port <0-
65535>|source-port-bitmark <0-65535>]
```

permit [<0-255>|tcp|udp]	Creates a permit rule and identifies the protocol type. This permit rule is applied only to packets matching the protocol specified here. • <0-255> – Identifies the protocol from its number. Specify the protocol number from 0 - 255. • tcp – Configures the protocol as TCP • udp – Configures the protocol as UDP
[<SOURCE-NETWORK-IP/MASK>| any| host <SOURCE-HOST-IP>]	Specifies the source IP address as *any*, *host*, or *network*. • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
[<DEST-NETWORK-IP/MASK>| any| host <DEST-HOST-IP>]	Specifies the destination IP address as *any*, *host*, or *network*. • <DEST-NETWORK-IP/MASK> – Configures a network as the destination. Provide the network's IPv4 address along with the mask. • host <DEST-HOST-IP> – Configures a single device as the destination. Provide the host device's IPv4 address. • any – Specifies that the destination can be any device

control-flag <0-63>	Configures the decimal number (representing a bit string) that specifies the control flag bits in byte 14 of the TCP header • <0-63> – Specify a value from 0 - 63. **Note:** Control flags can be used only in ACLs designed to filter TCP traffic. The TCP header contains several one-bit boolean fields known as flags that influence flow of data across a TCP connection. Ignoring the CWR and ECE flags added for congestion notification by RFC 3168, there are six TCP control flags. • URG flag - Marks incoming packet as urgent. • ACK flag - Acknowledges receipt of packet • PUSH flag - Ensures that the packet is given appropriate priority. Often used at the beginning and end of data transfer. • RST flag - Resets the connection. Happens when remote host receives a establish connection packet, but does not have a service waiting to answer and sends a reply with reset flag. • SYN flag - Establishes the 3-way handshake between two hosts • FIN flag - Tears down the connection established between two hosts via the 3-way SYN process
destination-port <0-65535>	Configures the protocol destination port to match. The destination protocol can be TCP, UDP or any other protocol identified by its number (<0-255>). • <0-65535> – Specify the destination port from 0 - 65535.
destination-port-bitmark <0-65535>	Configures the decimal number representing the protocol destination port bits to match • <0-65535> – Specify the destination port bits from 0 - 65535.
dscp <0-63>	Configures the DSCP priority level • <0-63> – Specify a value from 0 - 63. **Note:** If specifying DSCP priority, ip-precedence cannot be specified.
ex3500-time-range <TIME-RANGE-NAME>	Applies a periodic or absolute time range to this rule • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured). For information on configuring EX3500 time-range, see *ex3500*.
ip-precedence <0-7>	Configures the IP header precedence • <0-7> – Specify a value from 0 - 7.
source-port <0-65535>	Configures the protocol source port to match. The source protocol can be TCP, UDP or any other protocol identified by its number (<0-255>). • <0-65535> – Specify the source port from 0 - 65535.
source-port-bitmark <0-65535>	Configures the decimal number representing the protocol source port bits to match • <0-65535> – Specify the source port bits from 0 - 65535.
rule-precedence <1-128>	The following keywords are recursive and common to all of the above parameters: • rule-precedence – Assigns a precedence to this permit rule • <1-128> – Specify a value from 1 - 5000. **Note:** Lower the precedence higher is the priority. A rule with precedence 3 gets priority over a rule with precedence 4 and is applied first to packets.

Usage Guidelines

Use this command to permit traffic between networks/hosts based on the protocol type selected in the access list configuration. The following protocols are supported:

- TCP
- UDP
- <0-255> (any Internet protocol other than TCP, UDP, and ICMP)

Whenever the interface receives the packet, its content is checked against the ACEs in the ACL. It is allowed or denied based on the ACL configuration.

- Filtering TCP/UDP allows you to specify port numbers as filtering criteria

Example

The following example permits outgoing TCP packets from all sources within the 192.168.14.0 network to any destination, with the TCP control flag set to 16 (acknowledge):

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#permit tcp 192.168.14.0/24 any
control-flag 16 rule-precedence 2

nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
 permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

Related Commands

no	Removes a specified permit access rule from this IPv4 EX3500 extended ACL

11.5.3 no

ex3500-ext-access-list

Removes a deny or permit access rule from this IPv4 EX3500 extended ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

```
no [deny|permit] [<0-255>|tcp|udp] [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-
HOST-IP>] [<DEST-NETWORK-IP/MASK>|any|host <DEST-HOST-IP>] [control-flag <0-63>|
destination-port <0-65535>|destination-port-bitmark <0-65535>|dscp <0-63>|ex3500-
time-range <TIME-RANGE-NAME>|ip-precedence <0-63>|rule-precedence <1-128>|
source-port <0-65535>|source-port-bitmark <0-65535>]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes a deny or permit access rule based on the parameters passed

Usage Guidelines

The keyword 'control-flag <0-63>' is only applicable to ACL rules filtering TCP traffic.

Example

The following example shows the IPv4 EX3500 extended ACL 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
 permit tcp 192.168.14.0/24 any control-flag 16 rule-precedence 2
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#

nx9500-6C8809(config-ip-ex3500-ext-acl-test)#no permit tcp 192.168.14.0/24 any
control-flag 16 rule-precedence 2
```

The following example shows the IPv4 EX3500 extended ACL 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#show context
ip ex3500-ext-access-list test
 deny tcp 192.168.14.0/24 host 192.168.13.13 rule-precedence 1
nx9500-6C8809(config-ip-ex3500-ext-acl-test)#
```

11.6 ex3500-std-access-list

ACCESS-LIST

A EX3500 standard ACL is a policy-based ACL that contains a set of filter criteria and action that is applied to traffic originating from a specified source.

The following table summarizes IPv4 EX3500 standard ACL configuration commands:

NOTE: To implement the EX3500 standard ACL, apply it directly to a EX3500 device, or to an EX35XX profile. For more information, see *access-group*.

Table 11.6 *EX3500-Standard-Access-List-Config Commands*

Command	Description	Reference
deny	Creates a deny rule that rejects packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing deny rule.	*page 11-76*
permit	Creates a permit rule that allows packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing permit rule.	*page 11-77*
no	Removes a deny and/or a permit access rule from this IPv4 EX3500 extended ACL	*page 11-78*

11.6.1 deny

ex3500-std-access-list

Creates a deny rule that rejects packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing deny rule.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

```
deny [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range
<TIME-RANGE-NAME>}
```

Parameters

```
• deny [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range
<TIME-RANGE-NAME>}
```

deny [<SOURCE-NETWORK-IP/MASK>| any| host <SOURCE-HOST-IP>]	Creates a deny rule that rejects packets from a specified source or a network. Use one of the following options to specify the source: any, host, or network. • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
ex3500-time-range <TIME-RANGE-NAME>	Optional. Applies a periodic or absolute time range to this deny rule • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured). The ACL is triggered during the time period configured in the specified EX3500 time range. For information on configuring EX3500 time-range, see *ex3500*.

Example

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#deny 192.168.14.0/24

nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
 deny 192.168.13.0/24
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
```

Related Commands

no	Removes a specified deny access rule from this IPv4 EX3500 standard ACL

11.6.2 permit

ex3500-std-access-list

Creates a permit rule that allows packets from a specified source or sources. The source can be a single device or a range of devices within a specified network. Use this command to also edit an existing permit rule.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

```
permit [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range
<TIME-RANGE-NAME>}
```

Parameters

```
• permit [<SOURCE-NETWORK-IP/MASK>|any|host <SOURCE-HOST-IP>] {ex3500-time-range
<TIME-RANGE-NAME>}
```

permit [<SOURCE-NETWORK-IP/MASK>| any| host <SOURCE-HOST-IP>]	Creates a permit rule that allows packets from a specified source or a network. Use one of the following options to specify the source: any, host, or network. • <SOURCE-NETWORK-IP/MASK> – Configures a network as the source. Provide the network's IPv4 address along with the mask. • host <SOURCE-HOST-IP> – Configures a single device as the source. Provide the host device's IPv4 address. • any – Specifies that the source can be any device
ex3500-time-range <TIME-RANGE-NAME>	Optional. Applies a periodic or absolute time range to this deny rule • <TIME-RANGE-NAME> – Specify the time range name (should be existing and configured). The ACL is triggered during the time period configured in the specified EX3500 time range. For information on configuring EX3500 time-range, see *ex3500*.

Example

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#permit host 192.168.13.13 ex3500-
time-range EX3500_TimeRange_01

nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
 deny 192.168.14.0/24
 permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
```

Related Commands

no	Removes a specified permit access rule from this IPv4 EX3500 standard ACL

11.6.3 no

ex3500-std-access-list

Removes a deny or permit access rule from this IPv4 EX3500 standard ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510

Syntax

```
no [deny|permit] [<SOURCE-IP/MASK>|any|host <IP>] {ex3500-time-range <TIME-RANGE-NAME>}
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes a deny or permit access rule based on the parameters passed

Example

The following example shows the IPv4 EX3500 standard ACL 'test' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
 deny 192.168.14.0/24
 permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#

nx9500-6C8809(config-ip-ex3500-std-acl-test)#no deny 192.168.14.0/24
```

The following example shows the IPv4 EX3500 standard ACL 'test' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-ip-ex3500-std-acl-test)#show context
ip ex3500-std-access-list test
 permit host 192.168.13.13 ex3500-time-range EX3500_TimeRange_01
nx9500-6C8809(config-ip-ex3500-std-acl-test)#
```

12 DHCP-SERVER-POLICY

This chapter summarizes *Dynamic Host Control Protocols* (DHCP) server policy commands in the CLI command structure.

DHCP automatically assigns network IP addresses to requesting clients to enable them access to network resources. DHCP tracks IP address assignments, their lease times and their availability. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the controller's (wireless controller, service platform, or access point) onboard DHCP server allocates an address to a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, wireless clients (with assigned leases) are expected to renew them to continue using the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The controller's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). IP address management is conducted by a controller's DHCP server and not by an administrator.

The controller's internal DHCP server groups wireless clients based on defined user-class options. Clients with a defined set of user-class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnets. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Use the (config) instance to configure DHCP/DHCPv6 server policy parameters. To navigate to the config DHCP server policy instance, use the following commands:

```
<DEVICE>(config)#dhcp-server-policy <POLICY-NAME>

rfs6000-37FABE(config)#dhcp-server-policy test
rfs6000-37FABE(config-dhcp-server-policy-test)#

rfs6000-37FABE(config-dhcp-policy-test)#?
DHCP policy Mode commands:
  bootp         BOOTP specific configuration
  dhcp-class    Configure DHCP class (for address allocation using DHCP
                user-class options)
  dhcp-pool     Configure DHCP server address pool
  dhcp-server   Activating dhcp server based on criteria
  no            Negate a command or set its defaults
  option        Define DHCP server option
  ping          Specify ping parameters used by DHCP Server

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs6000-37FABE(config-dhcp-policy-test)#
```

To navigate to the config DHCPv6 server policy instance, use the following commands:

```
<DEVICE>(config)#dhcpv6-server-policy <POLICY-NAME>

rfs6000-37FABE(config)#dhcpv6-server-policy test
rfs6000-37FABE(config-dhcpv6-server-policy-test)#

rfs6000-37FABE(config-dhcpv6-server-policy-test)#?
DHCPv6 server policy Mode commands:
  dhcpv6-pool              Configure DHCPV6 server address pool
  no                       Negate a command or set its defaults
  option                   Define DHCPv6 server option
  restrict-vendor-options  Restrict vendor specific options to be sent in
                           server reply
  server-preference        Server preference value sent in the reply, by the
                           server to client

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs6000-37FABE(config-dhcpv6-server-policy-test)#
```

This chapter is organized as follows:

- *dhcp-server-policy*
- *dhcpv6-server-policy*

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

12.1 dhcp-server-policy

- *DHCP-SERVER-POLICY*

The following table summarizes DHCP server policy configuration commands:

Table 12.1 *DHCP-Server-Policy-Config Commands*

Command	Description	Reference
bootp	Configures a BOOTP specific configuration	*page 12-4*
dhcp-class	Configures a DHCP server class	*page 12-5*
dhcp-pool	Configures a DHCP server address pool	*page 12-11*
dhcp-server	Configures the activation-criteria that triggers dynamic activation of DHCP service running on a redundancy device	*page 12-56*
no	Negates a command or sets its default	*page 12-58*
option	Defines the DHCP option used in DHCP pools	*page 12-59*
ping	Specifies ping parameters used by a DHCP server	*page 12-60*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

12.1.1 bootp

dhcp-server-policy

Configures a BOOTP specific configuration

Bootstrap Protocol (BOOTP) requests are used by UNIX diskless workstations to obtain the location of their boot image and IP address within the managed network. A BOOTP configuration server provides this information and also assigns an IP address from a configured pool of IP addresses. By default, all BOOTP requests are forwarded to the BOOTP configuration server by the controller. When enabled, this feature allows controllers, using this DHCP server policy, to ignore BOOTP requests.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
bootp ignore
```

Parameters

```
• bootp ignore
```

bootp ignore	Enables controllers to ignore BOOTP requests

Example

```
rfs6000-37FABE(config-dhcp-policy-test)#bootp ignore

rfs6000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 bootp ignore
rfs6000-37FABE(config-dhcp-policy-test)#
```

Related Commands

no	Disables the ignore BOOTP requests option

12.1.2 dhcp-class

dhcp-server-policy

A controller, service platform, or access point's local DHCP server assigns IP addresses to requesting DHCP clients based on user class option names. The DHCP server can assign IP addresses from as many IP address ranges as defined by an administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

A DHCP user class applies different DHCP settings to a set of wireless clients. Wireless clients using the same DHCP settings are grouped under one DHCP class. Grouping users into classes facilitates the provision of differentiated service.

The following table summarizes DHCP class configuration commands:

Table 12.2 *DHCP-Class Config Commands*

Command	Description	Reference
dhcp-class	Creates a DHCP class and enters its configuration mode	*page 12-6*
dhcp-class-mode commands	Invokes DHCP class configuration commands	*page 12-7*

12.1.2.1 dhcp-class

dhcp-class

Creates a DHCP server class and enters its configuration mode. Use this command to configure user class option values. Once defined, the controller's internal DHCP server uses the configured values to group wireless clients into DHCP classes. Therefore, each user class consists of wireless clients sharing the same set of user class values.

You can also use this command to modify an existing DHCP user class settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp-class <DHCP-CLASS-NAME>
```

Parameters

- `dhcp-class <DHCP-CLASS-NAME>`

<DHCP-CLASS-NAME>	Creates a DHCP user class • <DHCP-CLASS-NAME> – Specify a name that appropriately identifies this class of wireless clients. If the class does not exist, it is created. The class name should not exceed 32 characters in length.

Example

```
rfs6000-37FABE(config-dhcp-policy-test)#dhcp-class dhcpclass1

rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#?
DHCP class Mode commands:
  multiple-user-class  Enable multiple user class option
  no                   Negate a command or set its defaults
  option               Configure DHCP Server options

  clrscr               Clears the display screen
  commit               Commit all changes made in this session
  do                   Run commands from Exec mode
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands

no	Removes a configured DHCP user class policy

12.1.2.2 dhcp-class-mode commands

dhcp-class

Use DHCP class mode commands to configure the parameters of the DHCP user class.

The following table summarizes DHCP user class configuration commands:

Table 12.3 *DHCP-Class-Config-Mode Commands*

Command	Description	Reference
multiple-user-class	Enables multiple user class option for this DHCP user class policy	*page 12-8*
no	Negates a command or sets its default	*page 12-9*
option	Configures DHCP user class options for this DHCP user class policy	*page 12-10*

12.1.2.2.1 multiple-user-class

dhcp-class-mode commands

Enables multiple user class option for this DHCP user class policy. Enabling this option allows this user class to transmit multiple option values to other DHCP servers also supporting multiple user class options.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
multiple-user-class
```

Parameters

None

Example

```
rfs6000-37FABE(config-dhcp-policy-test-class-class1)#multiple-user-class

rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
  multiple-user-class
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands

no	Disables the multiple user class option for the selected DHCP user class policy

12.1.2.2.2 no

dhcp-class-mode commands

Removes this DHCP user class policy's settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [multiple-user-class|option]
no option user-class <VALUE>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Disables multiple user class options on this DHCP user class policy

Example

The following example shows the DHCP class settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
  option user-class hex
  multiple-user-class
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#

rfs6000-37FABE(config-dhcp-policy-test-class-class1)#no multiple-user-class
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#no option user-class hex
```

The following example shows the DHCP class settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

12.1.2.2.3 option

dhcp-class-mode commands

Configures DHCP user class options for this DHCP user class policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
option user-class <VALUE>
```

Parameters

- `option user-class <VALUE>`

user-class <VALUE>	Configures DHCP user class options • <VALUE> – Specify the DHCP user class option's ASCII value.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-class-class1)#option user-class hex

rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#show context
 dhcp-class dhcpclass1
  option user-class hex
  multiple-user-class
rfs6000-37FABE(config-dhcp-policy-test-class-dhcpclass1)#
```

Related Commands

no	Removes the configured DHCP user class option

12.1.3 dhcp-pool

dhcp-server-policy

The DHCP pool command creates and manages a pool of IP addresses. These IP addresses are assigned to devices using the DHCP protocol. IP addresses have to be unique for each device in the network. Since IP addresses are finite, DHCP ensures that every device, in the network, is issued a unique IP address by tracking the issue, release, and reissue of IP addresses.

The DHCP pool command configures a finite set of IP addresses that can be assigned whenever a device joins a network.

The following table summarizes DHCP pool configuration mode commands:

Table 12.4 *DHCP-Pool-Config Commands*

Command	Description	Reference
dhcp-pool	Creates a DHCP pool and enters its configuration mode	*page 12-12*
dhcp-pool-mode commands	Summarizes DHCP pool configuration mode commands	*page 12-14*

12.1.3.1 dhcp-pool

dhcp-pool

Configures a DHCP server address pool

DHCP services are available for specific IP interfaces. A pool (or range) of IP network addresses and DHCP options can be created for each IP interface defined. This range of addresses is available to DHCP enabled wireless devices on either a permanent or leased basis. This enables the reuse of limited IP address resources for deployment in any network. DHCP options are provided to each DHCP client with a DHCP response and provides DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCP client.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp-pool <POOL-NAME>
```

Parameters

- `dhcp-pool <POOL-NAME>`

<POOL-NAME>	Creates a DHCP server address pool • <POOL-NAME> – Specify a name that appropriately identifies this DHCP address pool. If the pool does not exist, it is created. The pool name cannot be modified as part of the edit process. However, an obsolete address pool can be deleted.

Example

```
rfs6000-37FABE(config-dhcp-policy-test)#dhcp-pool pool1

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1)#?
DHCP pool Mode commands:
  address               Configure network pool's included addresses
  bootfile              Boot file name
  ddns                  Dynamic DNS Configuration
  default-router        Default routers
  dns-server            DNS Servers
  domain-name           Configure domain-name
  excluded-address      Prevent DHCP Server from assigning certain addresses
  lease                 Address lease time
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  network               Network on which DHCP server will be deployed
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  respond-via-unicast   Send DHCP offer and DHCP Ack as unicast messages
  static-binding        Configure static address bindings
  static-route          Add static routes to be installed on dhcp clients
  update                Control the usage of DDNS service
```

```
  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1)#
```

Related Commands

no	Removes a specified DHCP address pool

12.1.3.2 dhcp-pool-mode commands

dhcp-pool

Configures the DHCP pool parameters

The following table summarizes DHCP pool configuration commands:

Table 12.5 *DHCP-Pool-Config-Mode Commands*

Command	Description	Reference
address	Specifies a range of addresses for a DHCP address pool	*page 12-15*
bootfile	Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.	*page 12-17*
ddns	Configures dynamic DNS parameters	*page 12-18*
default-router	Configures a default router or gateway IP address for the network pool	*page 12-20*
dns-server	Sets a DNS server's IP address available to all DHCP clients connected to the DHCP pool	*page 12-22*
domain-name	Sets the domain name for the network pool	*page 12-24*
excluded-address	Prevents a DHCP server from assigning certain addresses to the DHCP pool	*page 12-25*
lease	Sets a valid lease for the IP address used by DHCP clients in the DHCP pool	*page 12-27*
netbios-name-server	Configures a NetBIOS (WINS) name server's IP address	*page 12-29*
netbios-node-type	Defines the NetBIOS node type	*page 12-30*
network	Configures the network on which the DHCP server is deployed	*page 12-31*
next-server	Configures the next server in the boot process	*page 12-32*
no	Negates a command or sets its default	*page 12-9*
option	Configures RAW DHCP options	*page 12-10*
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	*page 12-37*
static-route	Configures a static route for a DHCP pool	*page 12-36*
update	Controls the usage of the DDNS service	*page 12-38*
static-binding	Configures static address bindings	*page 12-39*

12.1.3.2.1 address

dhcp-pool-mode commands

Adds IP addresses to the DHCP address pool. These IP addresses are assigned to each device joining the network.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
address [<IP>|<HOST-ALIAS-NAME>|range]

address [<IP>|<HOST-ALIAS-NAME>|range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]] {class <DHCP-CLASS-NAME>}
```

Parameters

```
• address [<IP>|<HOST-ALIAS-NAME>|range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]] {class <DHCP-CLASS-NAME>}
```

<IP>	Adds a single IP address to the DHCP address pool
<HOST-ALIAS-NAME>	Adds a single host mapped to the specified host alias. The host alias should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host *'1.1.1.100'*. For more information, see *alias*.
range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]	Adds a range of IP addresses to the DHCP address pool. Use one of the following options to provide the first IP address in the range: • <START-IP> – Specifies the first IP address in the range • <START-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the first IP address in the range Use one of the following options to provide the last IP address in the range: • <END-IP> – Specifies the last IP address in the range • <END-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the last IP address in the range The host aliases should be existing and configured.
class <DHCP-CLASS-NAME>	Optional. Applies additional DHCP options, or a modified set of options to those available to wireless clients. For more information, see *dhcp-class*. • <DHCP-CLASS-NAME> – Sets the DHCP class.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#address 192.168.13.4 class
 dhcpclass1

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the DHCP pool's configured IP addresses
dhcp-class	Creates and configures the DHCP class parameters
alias	Creates and configures a network, VLAN, host, string, and network-service aliases

12.1.3.2.2 bootfile

dhcp-pool-mode commands

The Bootfile command provides a diskless node path to the image file while booting up. Only one file can be configured for each DHCP pool.

For more information on the BOOTP protocol with reference to the DHCP policy, see *bootp*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
bootfile <IMAGE-FILE-PATH>
```

Parameters

- `bootfile <IMAGE-FILE-PATH>`

<IMAGE-FILE-PATH>	Sets the path to the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#bootfile test.txt

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Resets the boot image path for BOOTP clients
bootp	Configures BOOTP protocol parameters

12.1.3.2.3 ddns

dhcp-pool-mode commands

Configures *Dynamic Domain Name Service* (DDNS) parameters. Dynamic DNS provides a way to access an individual device in a DHCP serviced network using a static device name.

Depending on the DHCP server's configuration, the IP address of a device changes periodically. To ensure continuous accessibility to a device (having a dynamic IP address), the device's current IP address is published to a DDNS server that resolves the static device name (used to access the device) with a changing IP address.

The DDNS server must be accessible from outside the network and must be configured as an address resolver.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ddns [domainname|multiple-user-class|server|ttl]

ddns domainname <DDNS-DOMAIN-NAME>
ddns multiple-user-class
ddns server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
ddns ttl <1-864000>
```

Parameters

- `ddns domainname <DDNS-DOMAIN-NAME>`

domainname <DDNS-DOMAIN-NAME>	Sets the domain name used for DNS updates The controller uses DNS to convert human readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *Fully Qualified Domain Name* (FQDN) consists of a host name plus a domain name. For example, computername.domain.com.

- `ddns multiple-user-class`

multiple-user-class	Enables the multiple user class options with this DDNS domain

- `ddns server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

server	Configures the DDNS server used by this DHCP profile
[<IP>|<HOST-ALIAS-NAME>]	Configures the primary DDNS server. This is the default server. Use one of the following options to specify the primary DDNS server: • <IP> – Specifies the primary DDNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DDNS server's IP address. The host alias should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DDNS server. If the primary server is not reachable, this server is used. Use one of the following options to identify the secondary DDNS server: • <IP> – Specifies the secondary DDNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the secondary DDNS server's IP address. The host alias should be existing and configured.

- `ddns ttl <1-864000>`

ttl <1-864000>	Configures the *Time To Live* (TTL) value for DDNS updates • <1-86400> – Specify a value from 1 - 864000 seconds.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns domainname WID

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns multiple-user-class

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#ddns server 192.168.13.9

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Resets or disables a DHCP pool's DDNS settings

12.1.3.2.4 default-router

dhcp-pool-mode commands

Configures a default router or gateway IP address for a network pool

After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address of one or a group of routers the controller uses to map host names into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

- `default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary default router, using one of the following options: • <IP> – Specifies the primary default router's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary default router, using one of the following options: • <IP1> – Specifies the secondary default router's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary default router's IP address. If the primary default router is unavailable, the secondary router is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host *'1.1.1.100'*. For more information, see *alias*. A maximum of 8 default routers can be configured.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#default-router 192.168.13.8
192.168.13.9

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the default router settings

12.1.3.2.5 dns-server

dhcp-pool-mode commands

Configures a network's DNS server. The DNS server supports all clients connected to networks supported by the DHCP server.

For DHCP clients, the DNS server's IP address maps the hostname to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

- `dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1> <HOST-ALIAS-NAME1>}`

[<IP>| <HOST-ALIAS-NAME>]	Configures the primary DNS server, using one of the following options:
	• <IP> – Specifies the primary DNS server's IP address
	• <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DNS server's IP address
	A maximum of 8 DNS servers can be configured.
	To enable redirection of DNS queries to OpenDNS it is necessary that the DNS server IP addresses provided here should point to the OpenDNS resolver (208.67.220.220 or 208.67.222.222). OpenDNS is a proxy DNS server that provides additional functionality, such as Web filtering, reporting, and performance enhancements in addition to DNS services. When configured on a WLAN, DNS queries from wireless clients are redirected to OpenDNS. The following example illustrates the configuration:
	`dhcp-server-policy dhcppolicy`
	`dhcp-pool dhcppool`
	`network 192.168.1.0/24`
	`address range 192.168.1.160 192.168.1.200`
	`default-router 192.168.1.105`
	`dns-server 208.67.220.220`
	Note, the above example shows the OpenDNS server as being 208.67.2202.220. The alternative IP address 208.67.222.222 can also be used.
	For more information on the entire configuration that needs to be done to integrate WiNG access point, controllers, and service platform with OpenDNS , see *opendns*.

{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DNS server, using one of the following options: • <IP1> – Specifies the secondary DNS server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary DNS server's IP address. If the primary DNS server is unavailable, the secondary server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host '*1.1.1.100*'. For more information, see *alias*. A maximum of 8 DNS servers can be configured.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#dns-server 192.168.13.19

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes DNS server settings

12.1.3.2.6 domain-name

dhcp-pool-mode commands

Sets the domain name for the DHCP pool. This is the domain name used by the controller with this pool.

Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. The FQDN consists of the host name and the domain name. For example, computername.domain.com.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
domain-name <DOMAIN-NAME>
```

Parameters

- `domain-name <DOMAIN-NAME>`

<DOMAIN-NAME>	Defines the DHCP pool's domain name

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#domain-name documentation

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes a DHCP pool's domain name

12.1.3.2.7 excluded-address

dhcp-pool-mode commands

Identifies a single IP address or a range of IP addresses, included in the DHCP address pool, that cannot be assigned to clients by the DHCP server

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
excluded-address [<IP>|<HOST-ALIAS-NAME>|range]

excluded-address <IP>
excluded-address <HOST-ALIAS-NAME>
excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]
```

Parameters

- `excluded-address <IP>`

<IP>	Adds a single IP address to the excluded address list

- `excluded-address <HOST-ALIAS-NAME>`

<HOST-ALIAS-NAME>	Adds a host alias. The host alias is mapped to a host's IP address. The host identified by the host alias is added to the excluded address list. The host alias should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host *'1.1.1.100'*. For more information, see *alias*.

- `excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-NAME>]`

range [<START-IP>| <START-HOST-ALIAS-NAME>] [<END-IP>| <END-HOST-ALIAS-NAME>]	Adds a range of IP addresses to the excluded address list. Use one of the following options to provide the first IP address in the range: • <START-IP> – Specifies the first IP address in the range • <START-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the first IP address in the range Use one of the following options to provide the last IP address in the range: • <END-IP> – Specifies the last IP address in the range • <END-HOST-ALIAS-NAME> – Specifies a host alias, mapped to the last IP address in the range The host aliases should be existing and configured.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#excluded-address range
192.168.13.25 192.168.13.28

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the exclude IP addresses settings

12.1.3.2.8 lease

dhcp-pool-mode commands

A lease is the duration a DHCP issued IP address is valid. Once a lease expires, and if the lease is not renewed, the IP address is revoked and is available for reuse. Generally, before an IP lease expires, the client tries to get the same IP address issued for the next lease period. This feature is enabled by default, with a lease period of 24 hours (1 day).

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
lease [<0-365>|infinite]

lease infinite
lease <0-365> {0-23} {0-59} {0-59}
```

Parameters

- `lease infinite`

infinite	The lease never expires (equal to a static IP address assignment)

- `lease <0-365> {<0-23>} {<0-59>} {<0-59>}`

<0-365>	Configures the lease duration in days **Note:** Days may be 0 only when hours and/or minutes are greater than 0.
<0-23>	Optional. Sets the lease duration in hours
<0-59>	Optional. Sets the lease duration in minutes
<0-59>	Optional. Sets the lease duration in seconds

Usage Guidelines

If lease parameter is not configured on the DHCP pool, the default is used. The default is 24 hours.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#lease 100 23 59 59

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Resets values or disables the DHCP pool lease settings

12.1.3.2.9 netbios-name-server

dhcp-pool-mode commands

Configures the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

- `netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary NetBIOS name server, using one of the following options: • <IP> – Specifies the primary NetBIOS name server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary NetBIOS name server, using one of the following options: • <IP1> – Specifies the secondary NetBIOS name server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary NetBIOS name server's IP address. If the primary NetBIOS name server is unavailable, the secondary server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host *'1.1.1.100'*. For more information, see *alias*.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-name-server
192.168.13.25

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the NetBIOS name server settings

12.1.3.2.10 netbios-node-type

dhcp-pool-mode commands

Defines the predefined NetBIOS node type. The NetBIOS node type resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

- `netbios-node-type [b-node|h-node|m-node|p-node]`

[b-node|h-node| m-node|p-node]	Defines the netbios node type • b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. • h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. • m-node – Sets the node type as mixed. A mixed node uses broadcast queries to find a node, and failing that, queries a known p-node name server for the address. • p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#netbios-node-type b-node

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the NetBIOS node type settings

12.1.3.2.11 network

dhcp-pool-mode commands

Configures the DHCP server's network settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
network [<IP/M>|<NETWORK-ALIAS-NAME>]
```

Parameters

- `network [<IP/M>|<NETWORK-ALIAS-NAME>]`

<IP/M>	Configures the network number and mask (for example, 192.168.13.0/24)
<NETWORK-ALIAS-NAME>	Configures a network alias to identify the network number and mask • <NETWORK-ALIAS-NAME> – Specify the network alias name. It should be existing and configured. A network alias defines a single network address. For example, 'alias network $NET 1.1.1.0/24'. In this example, the network alias name is: *$NET* and the network it is mapped to is: *1.1.1.0/24*. For more information, see *alias*.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#network 192.168.13.0/24

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the network number and mask configured for this DHCP pool

12.1.3.2.12 next-server

dhcp-pool-mode commands

Configures the next server in the boot process

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
next-server [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

- `next-server [<IP>|<HOST-ALIAS-NAME>]`

<IP>	Configures the next server's (the first server in the boot process) IP address
<HOST-ALIAS-NAME>	Configures a host alias, mapped to the next server's IP address • <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured. A host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#next-server 192.168.13.26

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes the next server configuration settings

12.1.3.2.13 no

dhcp-pool-mode commands

Removes or resets this DHCP user pool's settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [address|bootfile|ddns|default-router|dns-server|domain-name|excluded-
address|lease|netbios-name-server|netbios-node-type|network|next-server|option|
respond-via-unicast|static-binding|static-route|update]

no [bootfile|default-router|dns-server|domain-name|lease|netbios-name-server|
netbios-node-type|next-server|network|respond-via-unicast]


no address [<IP>|<HOST-ALIAS-NAME>|all]

no address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-HOST-ALIAS-
NAME>]

no ddns [domainname|multiple-user-class|server|ttl]

no excluded-address [<IP>|<HOST-ALIAS-NAME>]

no excluded-address range [<START-IP>|<START-HOST-ALIAS-NAME>] [<END-IP>|<END-
HOST-ALIAS-NAME>]

no option <OPTION-NAME>

no static-binding client-identifier <CLIENT-IDENTIFIER>

no static-binding hardware-address <MAC>

no static-route <IP/MASK> <GATEWAY-IP>

no update dns {override}
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or resets this DHCP user pool's settings

Example

The following example shows the DHCP pool settings before the 'no' commands are executed:

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  network 192.168.13.0/24
  address 192.168.13.4 class dhcpclass1
  lease 100 23 59 59
  ddns server 192.168.13.9
  ddns domainname WID
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  domain-name documentation
  netbios-node-type b-node
  bootfile test.txt
```

```
  default-router 192.168.13.8 192.168.13.9
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  next-server 192.168.13.26
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no bootfile
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no network
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no default-router
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no next-server
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no domain-name
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no ddns domainname
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#no lease
```

The following example shows the DHCP pool settings after the ‘no’ commands are executed:

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

12.1.3.2.14 option

dhcp-pool-mode commands

Configures raw DHCP options. The DHCP option must be configured under the DHCP server policy. The options configured under the DHCP pool/DHCP server policy can also be used in static-bindings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]
```

Parameters

- `option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]`

<OPTION-NAME>	Sets the name of the DHCP option
<DHCP-OPTION-IP>	Sets DHCP option as an IP address
<DHCP-OPTION-ASCII>	Sets DHCP option as an ASCII string

NOTE: An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show runnig config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#option option1
157.235.208.80

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Resets values or disables the DHCP pool option settings

12.1.3.2.15 static-route

dhcp-pool-mode commands

Configures a static route for a DHCP pool. Static routes define a gateway for traffic intended for other networks. This gateway is always used when an IP address does not match any route in the network.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
static-route <IP/M> <IP>
```

Parameters

- `static-route <IP/M> <IP>`

<IP/M>	Specifies the IP destination prefix (for example, 10.0.0.0/8)
<IP>	Specifies the gateway IP address

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-route 192.168.13.0/
24 192.168.13.7

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
  static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes static route settings

12.1.3.2.16 respond-via-unicast

dhcp-pool-mode commands

Sends DHCP offer and acknowledgement as unicast messages

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
respond-via-unicast
```

Parameters

None

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#respond-via-unicast

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Disables sending of a DHCP offer and DHCP Ack as unicast messages. When disabled, sends offer and acknowledgement as broadcast messages.

12.1.3.2.17 update

dhcp-pool-mode commands

Controls the use of the DDNS service

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
update dns {override}
```

Parameters

- `update dns {override}`

dns {override}	Configures Dynamic DNS parameters • override – Optional. Enables Dynamic DNS updates on an onboard DHCP server

Usage Guidelines

A DHCP client cannot perform updates for RR's A, TXT and PTR resource records. Use `update (dns) (override)` to enable the internal DHCP server to send DDNS updates for resource records. The DHCP server can override the client, even if the client is configured to perform the updates.

In the DHCP server's DHCP pool, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the DHCP server and the DNS server.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#update dns override

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  update dns override
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
  static-route 192.168.13.0/24 192.168.13.7
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

Related Commands

no	Removes dynamic DNS service control

12.1.3.3 static-binding

dhcp-pool-mode commands

Configures static IP address information for a particular device. Static address binding is executed on the device's hostname, client identifier, or MAC address. Static bindings allow the configuration of client parameters, such as DHCP server, DNS server, default routers, fixed IP address etc.

The following table summarizes static binding configuration commands:

Table 12.6 *Static-Binding-Config Commands*

Command	Description	Reference
static-binding	Creates a static binding policy and enters its configuration mode	*page 12-40*
static-binding-mode commands	Invokes static binding configuration commands	*page 12-42*

12.1.3.3.1 static-binding

static-binding

Configures static address bindings

A static address binding is a collection of configuration parameters, including an IP address, associated with, or bound to, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings assign IP addresses without creating numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
static-binding [client-identifier <CLIENT>|hardware-address <MAC>]
```

Parameters

- `static-binding [client-identifier <CLIENT>|hardware-address <MAC>]`

client-identifier <CLIENT>	Enables a static binding configuration for a client based on its client identifier (as provided by DHCP option 61 and its key value) • <CLIENT> – Specify the client identifier (DHCP option 61).
hardware-address <MAC>	Enables a static binding configuration for a client based on its MAC address • <MAC> – Specify the MAC address of the client.

Example

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#static-binding client-
identifier test

rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#show context
 dhcp-pool testPool
  address 192.168.13.4 class dhcpclass1
  update dns override
  ddns server 192.168.13.9
  ddns multiple-user-class
  excluded-address range 192.168.13.25 192.168.13.28
  netbios-node-type b-node
  dns-server 192.168.13.19
  netbios-name-server 192.168.13.25
  option option1 157.235.208.80
  respond-via-unicast
  static-route 192.168.13.0/24 192.168.13.7
  static-binding client-identifier test
rfs4000-229D58(config-dhcp-policy-test-pool-testPool)#
```

```
rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#?
DHCP static binding Mode commands:
  bootfile              Boot file name
  client-name           Client name
  default-router        Default routers
  dns-server            DNS Servers
  domain-name           Configure domain-name
  ip-address            Fixed IP address for host
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  respond-via-unicast   Send DHCP offer and DHCP Ack as unicast messages
  static-route          Add static routes to be installed on dhcp clients

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs4000-229D58(config-dhcp-policy-test-pool-testPool-binding-test)#

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1)#static-binding hardware-
address
11-22-33-44-55-66
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#?
DHCP static binding Mode commands:
  bootfile              Boot file name
  client-name           Client name
  default-router        Default routers
  dns-server            DNS Servers
  domain-name           Configure domain-name
  ip-address            Fixed IP address for host
  netbios-name-server   NetBIOS (WINS) name servers
  netbios-node-type     NetBIOS node type
  next-server           Next server in boot process
  no                    Negate a command or set its defaults
  option                Raw DHCP options
  respond-via-unicast   Send DHCP offer and DHCP Ack as unicast messages
  static-route          Add static routes to be installed on dhcp clients

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#
```

Related Commands

no	Resets values or disables the DHCP policy static binding settings
static-binding-mode commands	Invokes static binding configuration commands

12.1.3.3.2 static-binding-mode commands

static-binding

The following table summarizes static binding configuration mode commands:

Table 12.7 *Static-Binding-Config-Mode Commands*

Command	Description	Reference
bootfile	Assigns a Bootfile name for the DHCP configuration on the network pool	*page 12-43*
client-name	Configures a client name	*page 12-44*
default-router	Configures default router or gateway IP address	*page 12-45*
dns-server	Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool	*page 12-46*
domain-name	Sets the network pool's domain name	*page 12-47*
ip-address	Configures a host's fixed IP address	*page 12-48*
netbios-name-server	Configures a NetBIOS (WINS) name server IP address	*page 12-49*
netbios-node-type	Defines the NetBIOS node type	*page 12-50*
next-server	Specifies the next server used in the boot process	*page 12-51*
no	Negates a command or sets its default	*page 12-52*
option	Configures raw DHCP options	*page 12-53*
respond-via-unicast	Sends a DHCP offer and DHCP Ack as unicast messages	*page 12-54*
static-route	Adds static routes installed on DHCP clients	*page 12-55*

12.1.3.3.3 bootfile

static-binding-mode commands

The Bootfile command provides a diskless node the path to the image file used while booting up. Only one file can be configured for each static IP binding.

For more information on the BOOTP protocol with reference to static binding, see *bootp*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
bootfile <IMAGE-FILE-PATH>
```

Parameters

- `bootfile <IMAGE-FILE-PATH>`

<IMAGE-FILE-PATH>	Sets the path to the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#bootfile test.txt

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   bootfile test.txt
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings
bootp	Configures BOOTP protocol parameters

12.1.3.3.4 client-name

static-binding-mode commands

Configures the client's name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
client-name <NAME>
```

Parameters

- `client-name <NAME>`

<NAME>	Specify the name of the client using this static IP address host pool. Do not include the domain name.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#client-name RFID

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   bootfile test.txt
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.5 default-router

static-binding-mode commands

Configures a default router or gateway IP address for the static binding configuration

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

- `default-router [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary default router, using one of the following options: • <IP> – Specifies the primary default router's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary default router's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary default router, using one of the following options: • <IP1> – Specifies the secondary default router's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary default router's IP address. If the primary default router is unavailable, the secondary router is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see alias.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#default-router
172.16.10.8 172.16.10.9

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.6 dns-server

static-binding-mode commands

Configures the DNS server for this static binding configuration. This DNS server supports the client for which the static binding has been configured.

For this client, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based on the order (sequence) configured.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

- `dns-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary DNS server, using one of the following options: • <IP> – Specifies the primary DNS server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary DNS server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary DNS server, using one of the following options: • <IP1> – Specifies the secondary DNS server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary DNS server's IP address. If the primary DNS server is unavailable, the secondary DNS server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see *alias*.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#dns-server
172.16.10.7

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.7 domain-name

static-binding-mode commands

Sets the domain name for the static binding configuration

Domain names are not case sensitive and contain alphabetic or numeric letters (or a hyphen). A fully qualified domain name (FQDN) consists of a host name plus a domain name. For example, computername.domain.com

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
domain-name <DOMAIN-NAME>
```

Parameters

- `domain-name <DOMAIN-NAME>`

<DOMAIN-NAME>	Defines the domain name for the static binding configuration

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#domain-name
documentation

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables the DHCP pool static binding settings

12.1.3.3.8 ip-address

static-binding-mode commands

Configures a fixed IP address for a host

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip-address [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

- `ip-address [<IP>|<HOST-ALIAS-NAME>]`

<IP>	Configures a fixed IP address (in dotted decimal format) of the client using this host pool
<HOST-ALIAS-NAME>	Configures a host alias identifying the fixed IP address of the client using this host pool A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host '*1.1.1.100*'. For more information, see *alias*.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#ip-address
172.16.10.9

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.9 netbios-name-server

static-binding-mode commands

Configures the NetBIOS (WINS) name server's IP address. This server is used to resolve NetBIOS host names.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}
```

Parameters

- `netbios-name-server [<IP>|<HOST-ALIAS-NAME>] {<IP1>|<HOST-ALIAS-NAME1>}`

[<IP>|<HOST-ALIAS-NAME>]	Configures the primary NetBIOS server, using one of the following options: • <IP> – Specifies the primary NetBIOS name server's IP address • <HOST-ALIAS-NAME> – Specifies a host alias, mapped to the primary NetBIOS name server's IP address
{<IP1>|<HOST-ALIAS-NAME1>}	Optional. Configures the secondary NetBIOS name server, using one of the following options: • <IP1> – Specifies the secondary NetBIOS name server's IP address • <HOST-ALIAS-NAME1> – Specifies a host alias, mapped to the secondary NetBIOS name server's IP address. If the primary NetBIOS name server is unavailable, the secondary server is used. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is '$HOST' and it maps to a single host '1.1.1.100'. For more information, see *alias*.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-name-
server 172.16.10.23

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.10 netbios-node-type

static-binding-mode commands

Configures different predefined NetBIOS node types. The NetBIOS node defines the way a device resolves NetBIOS names to IP addresses.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
netbios-node-type [b-node|h-mode|m-node|p-node]
```

Parameters

- `netbios-node-type [b-node|h-node|m-node|p-node]`

[b-node|h-mode| m-node|p-node]	Defines the netbios node type • b-node – Sets the node type as broadcast. Uses broadcasts to query nodes on the network for the owner of a NetBIOS name. • h-node – Sets the node type as hybrid. Uses a combination of two or more nodes. • m-node – Sets the node type as mixed. A mixed node uses broadcast queries to find a node, and failing that, queries a known p-node name server for the address. • p-node – Sets the node type as peer-to-peer. Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#netbios-node-
type
b-node

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.11 next-server

static-binding-mode commands

Configures the next server utilized in the boot process

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
next-server [<IP>|<HOST-ALIAS-NAME>]
```

Parameters

- `next-server [<IP>|<HOST-ALIAS-NAME>]`

<IP>	Configures the next server's (the first server in the boot process) IP address
<HOST-ALIAS-NAME>	Configures a host alias, mapped to the next server's IP address • <HOST-ALIAS-NAME> – Specify the host alias name. It should be existing and configured. A network host alias maps a name to a single network host. For example, 'alias host $HOST 1.1.1.100'. In this example the host alias is *'$HOST'* and it maps to a single host *'1.1.1.100'*. For more information, see *alias*.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#next-server
172.16.10.24

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.12 no

static-binding-mode commands

Negates or reverts static binding settings for the selected DHCP server policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [bootfile|client-name|default-router|dns-server|domain-name|ip-address|
netbios-name-server|netbios-node-type|next-server|option|respond-via-unicast|
static-route]

no option <OPTION-NAME>

no static-route <IP/MASK> <GATEWAY-IP>
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates or reverts static binding settings for the selected DHCP server policy

Example

The following example shows the DHCP pool static binding settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   ip-address 172.16.10.9
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   bootfile test.txt
   default-router 172.16.10.8 172.16.10.9
   dns-server 172.16.10.7
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no bootfile
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no ip-address
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no default-router
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#no dns-server
```

The following example shows the DHCP pool static binding settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

12.1.3.3.13 option

static-binding-mode commands

Configures the raw DHCP options in the DHCP policy. The DHCP options can be used only in static bindings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]
```

Parameters

- `option <OPTION-NAME> [<DHCP-OPTION-IP>|<DHCP-OPTION-ASCII>]`

<OPTION-NAME>	Sets the DHCP option name
<DHCP-OPTION-IP>	Sets the DHCP option as an IP address
<DHCP-OPTION-ASCII>	Sets the DHCP option as an ASCII string

Usage Guidelines

Defines non standard DHCP option codes (0-254)

NOTE: An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (Use `show running config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#option option1
172.16.10.10

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
   option option1 172.16.10.10
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

12.1.3.3.14 respond-via-unicast

static-binding-mode commands

Sends a DHCP offer and DHCP acknowledge as unicast messages

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
respond-via-unicast
```

Parameters

None

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#respond-via-
unicast

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
   option option1 172.16.10.10
   respond-via-unicast
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static binding settings

12.1.3.3.15 static-route

static-binding-mode commands

Adds static routes to the static binding configuration

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
static-route <IP/MASK> <GATEWAY-IP>
```

Parameters

- `static-route <IP/MASK> <GATEWAY-IP>`

<IP/MASK>	Sets the subnet for which the static route is configured
<GATEWAY-IP>	Specify the gateway's IP address

Example

```
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-1)#static-route
10.0.0.0/10 157.235.208.235

rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#show context
  static-binding client-identifier test
   client-name RFID
   domain-name documentation
   netbios-node-type b-node
   netbios-name-server 172.16.10.23
   next-server 172.16.10.24
   option option1 172.16.10.10
   respond-via-unicast
   static-route 10.0.0.0/10 157.235.208.235
rfs6000-37FABE(config-dhcp-policy-test-pool-pool1-binding-test)#
```

Related Commands

no	Resets values or disables DHCP pool static route settings

12.1.4 dhcp-server

dhcp-server-policy

Configures the activation-criteria (run-criteria) that triggers dynamic activation of DHCP service running on a redundancy device

In a managed wireless network, when the primary, active DHCP server fails (is unreachable), network clients are unable to access DHCP services, such as new IP address leasing and renewal of existing IP address leases. In such a scenario, the activation-criteria, when configured, triggers dynamic activation of the secondary DHCP server, allowing network clients to continue accessing DHCP services. The WiNG implementation provides activation-criteria options specific to a RF Domain, cluster setup, and a *Virtual Router Redundancy Protocol* (VRRP) master/client setup.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master]
```

Parameters

- `dhcp-server activation-criteria [cluster-master|rf-domain-manager|vrrp-master]`

dhcp-server	Enables dynamic activation of the DHCP server, running on a redundancy device, based on the activation criteria specified
activation-criteria [cluster-master| rf-domain-manager| vrrp-master]	Configures the activation criteria. Specify one of the following options as the activation criteria: • cluster-master – Configures the cluster-master criteria in a cluster setup. Within a cluster, DHCP service is enabled on the cluster master. While it remains disabled on the other cluster members. In case of the cluster master failing, the cluster-master activation criteria, when configured, triggers dynamic activation of DHCP service on the new cluster master. • rf-domain-manger – Configures the rf-domain-manager criteria on an RF Domain. Within a RF Domain, DHCP service is enabled on the RF Domain manager. While it remains disabled on the other devices within the RF Domain. In case of the RF Domain manager failing, the rf-domain-manager activation criteria, when configured, triggers dynamic activation of DHCP service on the new RF Domain manager. • vrrp-master – Configures the vrrp-master criteria within a VRRP master/client setup. In such a setup, the DHCP service is enabled on the VRRP master. While it remains disabled on the other members. In case of the VRRP master failing, the vrrp-master activation criteria, when configured, triggers dynamic activation of DHCP service on the new VRRP master.

Example

```
rfs4000-229D58(config-dhcp-policy-test)#dhcp-server activation-criteria rf-
domain-manager

rfs4000-229D58(config-dhcp-policy-test)#show context
dhcp-server-policy test
 dhcp-server activation-criteria rf-domain-manager
rfs4000-229D58(config-dhcp-policy-test)#

rfs4000-229D58(config-dhcp-policy-test)#no dhcp-server activation-criteria

rfs4000-229D58(config-dhcp-policy-test)#show context
dhcp-server-policy test
rfs4000-229D58(config-dhcp-policy-test)#
```

Related Commands

no	Removes the DHCP service activation criteria configured on this DHCP server policy

12.1.5 no

dhcp-server-policy

Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [bootp|dhcp-class|dhcp-pool|dhcp-server|option|ping]

no bootp ignore

no dhcp-class <DHCP-CLASS-NAME>

no dhcp-pool <DHCP-POOL-NAME>

no dhcp-server activation-criteria

no option <DHCP-OPTION>

no ping timeout
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or sets its default. When used in the DHCP server configuration context, the 'no' command resets or reverts the DHCP server policy settings

Example

The following example shows the DHCP policy 'test' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 bootp ignore
 dhcp-class dhcpclass1
 dhcp-pool pool1
  address 1.2.3.4 class dhcpclass1
  update dns override
  --More--
rfs6000-37FABE(config-dhcp-policy-test)#

rfs6000-37FABE(config-dhcp-policy-test)#no bootp ignore
rfs6000-37FABE(config-dhcp-policy-test)#no dhcp-class dhcpclass1
rfs6000-37FABE(config-dhcp-policy-test)#no dhcp-pool pool1
```

The following example shows the DHCP policy 'test' settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
rfs6000-37FABE(config-dhcp-policy-test)#
```

12.1.6 option

dhcp-server-policy

Configures raw DHCP options. The DHCP option has to be configured in the DHCP server policy. The options configured in the DHCP pool/DHCP server policy can also be used in static bindings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
option <OPTION-NAME> <0-254> [ascii|hexstring|ip]
```

Parameters

- `option <OPTION-NAME> <0-254> [ascii|hexstring|ip]`

<OPTION-NAME>	Configures the option name
<0-254>	Configures the DHCP option code from 0 - 254
ascii	Configures the DHCP option as an ASCII string
hexstring	Configures the DHCP option as a hexadecimal string
ip	Configures the DHCP option as an IP address

Usage Guidelines

Defines non standard DHCP option codes (0-254)

NOTE: An option name in ASCII format accepts a backslash (\) as an input, but is not displayed in the output (Use `show running config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs6000-37FABE(config-dhcp-policy-test)#option option1 200 ascii

rfs6000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 option option1 200 ascii
rfs6000-37FABE(config-dhcp-policy-test)#
```

Related Commands

no	Removes DHCP server options

12.1.7 ping

dhcp-server-policy

Configures the DHCP server's ping timeout interval. The controller uses the timeout to intermittently ping and discover whether a client requested IP address is available or in use.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ping timeout <1-10>
```

Parameters

- `ping timeout <1-10>`

timeout <1-10>	Sets the ping timeout from 1 - 10 seconds. The default is 1 second.

Example

```
rfs6000-37FABE(config-dhcp-policy-test)#ping timeout 2

rfs6000-37FABE(config-dhcp-policy-test)#show context
dhcp-server-policy test
 ping timeout 2
 option option1 200 ascii
rfs6000-37FABE(config-dhcp-policy-test)#
```

Related Commands

no	Resets the ping interval to 1 second

12.2 dhcpv6-server-policy

DHCP-SERVER-POLICY

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

The following table summarizes DHCPv6 server policy configuration commands:

Table 12.8 *DHCPv6-Server-Policy-Config Commands*

Command	Description	Reference
dhcpv6-pool	Creates a DHCPv6 pool and enters its configuration mode	*page 12-62*
option	Configures this DHCPv6 server policy's DHCP option settings, such as enterprise (vendor ID)	*page 12-73*
restrict-vendor-options	Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy	*page 12-75*
server-preference	Configures this DHCP server's preference value. This value is sent in DHCP server replies to the IPv6 client.	*page 12-76*
no	Negates or reverts this DHCPv6 server policy's settings	*page 12-77*

12.2.1 dhcpv6-pool

dhcpv6-server-policy

The following table summarizes DHCPv6 pool configuration mode commands:

Table 12.9 *DHCPv6-Pool-Config Commands*

Command	Description	Reference
dhcpv6-pool	Creates a DHCPv6 pool and enters its configuration mode	*page 12-63*
dhcpv6-pool-mode commands	Summarizes DHCPv6 pool configuration mode commands	*page 12-65*

12.2.1.1 dhcpv6-pool

dhcpv6-pool

Configures a DHCPv6 server address pool and enters its configuration mode

A DHCPv6 IPv6 pool is a resource from which IPv6 formatted addresses can be issued on DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcpv6-pool <POOL-NAME>
```

Parameters

- `dhcpv6-pool <POOL-NAME>`

<POOL-NAME>	Creates a DHCPv6 server address pool • <POOL-NAME> – Specify a name that appropriately identifies this DHCPv6 address pool. If the pool does not exist, it is created. The pool name cannot be modified as part of the edit process. However, an obsolete address pool can be deleted.

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test)#dhcpv6-pool DHCPv6Pool1

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#?
DHCPv6 pool Mode commands:
  dns-server     DNS Servers
  domain-name    Configure domain-name
  network        Network on which DHCPv6 server will be deployed
  no             Negate a command or set its defaults
  option         Raw DHCPv6 options
  refresh-time   Upper limit specifying the timer for which client should wait
                 before refreshing information
  sip            SIP server options

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
  write          Write running configuration to memory or terminal

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

```
rfs6000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test)#
```

Related Commands

no	Removes the DHCPv6 pool identified by the <POOL-NAME> keyword

12.2.1.2 dhcpv6-pool-mode commands

dhcpv6-pool

Configures the DHCPv6 pool parameters

The following table summarizes DHCPv6 pool configuration commands:

Table 12.10 *DHCPv6-Pool-Config-Mode Commands*

Command	Description	Reference
dns-server	Configures this DHCPv6 pool's DNS server	*page 12-66*
domain-name	Configures this DHCPv6 pool's domain name	*page 12-67*
network	Configures this DHCPv6 pool's network	*page 12-68*
option	Configures this DHCPv6 pool's raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool.	*page 12-70*
refresh-time	Configures this DHCPv6 pool's refresh time in seconds	*page 12-71*
sip	Configures this DHCPv6 pool's *Session Initiation Protocol* (SIP) server setting	*page 12-72*
no	Negates or reverts this DHCPv6 pool's settings	*page 12-69*

12.2.1.2.1 dns-server

dhcpv6-pool-mode commands

Configures this DHCPv6 pool's DNS server. The DNS server supports all clients connected to networks supported by the DHCPv6 server.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dns-server <IPv6> {<SECONDARY-IPv6>}
```

Parameters

- `dns-server <IPv6> {<SECONDARY-IPv6>}`

<IPv6>	Configures the primary DNS server's IPv6 address • <IPv6> – Specify the DNS server's IPv6 address (the server associated with this DHCP pool).
<SECONDARY-IPv6>	Configures the secondary DNS server's IPv6 address • <SECONDARY-IPv6> – Specify the secondary DNS server's IPv6 address (the server associated with this DHCP pool).

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#dns-server
2002::1

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

no	Removes this DHCPv6 pool's configured DNS server settings

12.2.1.2.2 domain-name

dhcpv6-pool-mode commands

Configures this DHCPv6 pool's domain name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
domain-name <DOMAIN-NAME>
```

Parameters

- `domain-name <DOMAIN-NAME>`

<DOMAIN-NAME>	Specify the DHCP pool's hostname or hostnames of the domain or domains

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#domain-name
TechPubs

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  domain-name TechPubs
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

no	Removes this DHCPv6 pool's domain name

12.2.1.2.3 network

dhcpv6-pool-mode commands

Configures this DHCPv6 pool's network. Use this command to configure the address of the network on which this DHCP server is deployed.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
network [<IPv6/M>|<NETWORK-ALIAS-NAME>]
```

Parameters

- `network [<IPv6/M>|<NETWORK-ALIAS-NAME>]`

<IPv6/M>	Specify this DHCPv6 pool network's IPv6 address and mask (for example, 1:2::1:0/96)
<NETWORK-ALIAS-NAME>	Specify this DHCPv6 pool network's alias name

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#network
2002::0/64

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

no	Removes the network IPv6 address and mask configured for this DHCPv6 pool

12.2.1.2.4 no

dhcpv6-pool-mode commands

Negates a command or sets its default. When used in the DHCPv6 pool configuration context, the 'no' command resets or reverts the DHCPv6 pool's settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [dns-server|domain-name|network|option|refresh-time|sip]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or sets its default. When used in the DHCPv6 pool configuration context, the 'no' command resets or reverts the DHCPv6 pool's settings.

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  refresh-time 1000
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
  option DHCPv6Pool1Option 60
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#no option
DHCPv6Pool1Option

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#no refresh-time

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

12.2.1.2.5 option

dhcpv6-pool-mode commands

Configures this DHCPv6 pool's raw DHCPv6 options. This is the vendor-specific option used in this DHCPv6 pool.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
option <OPTION-NAME> [<DHCPv6-OPTION-IP>|<DHCPv6-OPTION-ASCII>]
```

Parameters

- `option <OPTION-NAME> [<DHCPv6-OPTION-IP>|<DHCPv6-OPTION-ASCII>]`

<OPTION-NAME>	Sets the name of the DHCPv6 option
<DHCPv6-OPTION-IP>	Sets DHCPv6 option as an IPv6 address
<DHCPv6-OPTION-ASCII>	Sets DHCPv6 option as an ASCII string

NOTE: An option name in ASCII format accepts backslash (\) as an input but is not displayed in the output (Use `show running config` to view the output). Use a double backslash to represent a single backslash.

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#option
DHCPv6Pool1Option 60

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  dns-server 2002::1
  option DHCPv6Pool1Option 60
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

no	Removes this DHCPv6 pool's DHCP option settings

12.2.1.2.6 refresh-time

dhcpv6-pool-mode commands

Configures this DHCPv6 pool's refresh time in seconds. This is the interval between two successive DHCP pool refreshes. The DHCP refresh process refreshes IPv6 client information.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
refresh-time <600-4294967295>
```

Parameters

- `refresh-time <600-4294967295>`

refresh-time <600-4294967295>	Specify this DHCPv6 pool's refresh time from 600 -4294967295 seconds.

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#refresh-time
1000

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  refresh-time 1000
  domain-name TechPubs
  dns-server 2002::1
  option DHCPv6Pool1Option 60
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

no	Removes or reverts the configured DHCPv6 pool's refresh time

12.2.1.2.7 sip

dhcpv6-pool-mode commands

Configures this DHCPv6 pool's *Session Initiation Protocol* (SIP) server setting

Configures the domain name or domain names associated with the SIP servers. The SIP server is used to prioritize voice and video traffic on the network. SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several components (user agents, proxy servers, redirect servers, and registrars). User agents can contain SIP clients; proxy servers always contain SIP clients.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
sip [address <IPv6>|domain-name <DOMAIN-NAME>]
```

Parameters

- `sip [address <IPv6>|domain-name <DOMAIN-NAME>]`

sip [address <IPv6>|domain-name <DOMAIN-NAME>]	Configures the SIP server's setting, such as address and/or domain name

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#sip domain-name
TechPubsSIP

rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#show context
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  refresh-time 1000
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
  option DHCPv6Pool1Option 60
rfs6000-37FABE(config-dhcpv6-server-policy-test-pool-DHCPv6Pool1)#
```

Related Commands

no	Removes this DHCPv6 pool's SIP server setting

12.2.2 option

dhcpv6-server-policy

Configures this DHCPv6 server policy's DHCP option settings, such enterprise (vendor) ID

DHCPv6 services are available for specific IP interfaces. A pool (or range) of IPv6 network addresses and DHCPv6 options can be created for each IPv6 interface defined. This range of addresses can be made available to DHCPv6 enabled devices on either a permanent or leased basis. DHCPv6 options are provided to each client with a DHCPv6 response and provide DHCPv6 clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCPv6 client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCPv6 client.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
option <OPTION-NAME> <0-254> [ascii|hexstring|ipv6] <1-4294967295>
```

Parameters

- `option <OPTION-NAME> <0-254> [ascii|hexstring|ipv6] <1-4294967295>`

option <OPTION-NAME>	Specify a unique name for this DHCP option. The name should describe option's function.
<0-254>	Specify a DHCP option code for this option. • <0-254> – Specify a value from 0 -254. The system allows only one code, of the same value, for each DHCP option used in each DHCPv6 server policy.
ascii	Specifies the option type as ASCII (sends an ASCII compliant string to the client)
hexstring	Specifies the option type as a string of hexadecimal characters (sends a hexadecimal string to the client)
ipv6	Specifies the option type as IPv6 address (sends an IPv6 compatible address to the client)
<1-4294967295>	This parameter is common to all option types. • <1-4294967295> – Specifies the enterprise (vendor) ID. Specify a value from 1 - 4294967295. The option code (1) is reserved for subnet-mask and cannot be used. Each vendor should have a unique vendor ID used by the DHCP server to issue vendor-specific DHCP options.

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test)#option DHCPServerOption1 10
ascii 50

rfs6000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test)#
```

Related Commands

no	Removes the DHCPv6 server option settings configured for this DHCPv6 server policy

12.2.3 restrict-vendor-options

dhcpv6-server-policy

Restricts the use of vendor-specific DHCP options on this DHCPv6 server policy. When restricted, vendor-specific DHCP options, configured on this DHCPv6 server policy, are not included in the DHCPv6 server replies to IPv6 clients.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
restrict-vendor-options
```

Parameters

None

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test)#restrict-vendor-options

rfs6000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
 restrict-vendor-options
rfs6000-37FABE(config-dhcpv6-server-policy-test)#
```

Related Commands

no	Removes restriction on sending of vendor-specific options in DHCPv6 server replies to IPv6 clients

12.2.4 server-preference

dhcpv6-server-policy

Configures this DHCPv6 server's preference value. When configured, the server preference value is included in the DHCPv6 server's replies to IPv6 clients.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
server-preference <0-255>
```

Parameters

- `server-preference <0-255>`

server-preference <0-255>	Configures this DHCP server's preference value • <0-255> – Specify a value from 0 - 255.

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test)#server-preference 1

rfs6000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
 server-preference 1
 restrict-vendor-options
rfs6000-37FABE(config-dhcpv6-server-policy-test)#
```

Related Commands

no	Removes this DHCPv6 server's preference value

12.2.5 no

dhcpv6-server-policy

Negates or reverts this DHCPv6 server policy's settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [dhcpv6-pool|option|restrict-vendor-options|server-preference]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates or reverts this DHCPv6 server policy's settings

Example

```
rfs6000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
 server-preference 1
 restrict-vendor-options
rfs6000-37FABE(config-dhcpv6-server-policy-test)#

rfs6000-37FABE(config-dhcpv6-server-policy-test)#no restrict-vendor-options
rfs6000-37FABE(config-dhcpv6-server-policy-test)#no server-preference

rfs6000-37FABE(config-dhcpv6-server-policy-test)#show context
dhcpv6-server-policy test
 option DHCPServerOption1 10 ascii 50
 dhcpv6-pool DHCPv6Pool1
  network 2002::/64
  domain-name TechPubs
  sip domain-name TechPubsSIP
  dns-server 2002::1
rfs6000-37FABE(config-dhcpv6-server-policy-test)#
```

13 FIREWALL-POLICY

This chapter summarizes the firewall policy commands in the CLI command structure.

A firewall protects a network from attacks and unauthorized access from outside the network. Simultaneously, it allows authorized users to access required resources. Firewalls work on multiple levels. Some work at layers 1, 2 and 3 to inspect each packet. The packet is either passed, dropped or rejected based on rules configured on the firewall.

Firewalls use application layer filtering to enforce compliance. These firewalls can understand applications and protocols and can detect if an unauthorized protocol is being used, or an authorized protocol is being abused in any malicious way.

The third set of firewalls, 'Stateful Firewalls', consider the placement of individual packets within each packet in the series of packets being transmitted. If there is a packet that does not fit into the sequence, it is automatically identified and dropped.

Use (config) instance to configure firewall policy commands. To navigate to the *config-fw-policy* instance, use the following commands:

```
<DEVICE>(config)#firewall-policy <POLICY-NAME>

rfs6000-37FABE(config)#firewall-policy test
rfs6000-37FABE(config-fw-policy-test)#?
Firewall policy Mode commands:
  acl-logging                     Log on flow creating traffic
  alg                             Enable ALG
  clamp                           Clamp value
  dhcp-offer-convert              Enable conversion of broadcast dhcp offers to
                                  unicast
  dns-snoop                       DNS Snooping
  firewall                        Wireless firewall
  flow                            Firewall flow
  ip                              Internet Protocol (IP)
  ip-mac                          Action based on ip-mac table
  ipv6                            Internet Protocol version 6 (IPv6)
  ipv6-mac                        Action based on ipv6-mac table
  logging                         Firewall enhanced logging
  no                              Negate a command or set its defaults
  proxy-arp                       Enable generation of ARP responses on behalf
                                  of another device
  proxy-nd                        Enable generation of ND responses (for IPv6)
                                  on behalf of another device
  stateful-packet-inspection-l2   Enable stateful packet inspection in layer2
                                  firewall
  storm-control                   Storm-control
  virtual-defragmentation         Enable virtual defragmentation for IPv4
                                  packets (recommended for proper functioning
                                  of firewall)

  clrscr                          Clears the display screen
  commit                          Commit all changes made in this session
  do                              Run commands from Exec mode
  end                             End current mode and change to EXEC mode
  exit                            End current mode and down to previous mode
  help                            Description of the interactive help system
  revert                          Revert changes
  service                         Service Commands
  show                            Show running system information
  write                           Write running configuration to memory or
                                  terminal
rfs6000-37FABE(config-fw-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

13.1 firewall-policy

- *FIREWALL-POLICY*

The following table summarizes default firewall policy configuration commands:

Table 13.1 *Firewall-Policy-Config Commands*

Command	Description	Reference
acl-logging	Enables logging on flow creating traffic	*page 13-4*
alg	Enables an algorithm	*page 13-5*
clamp	Sets a clamp value to limit TCP MSS to inner path-MTU for tunnelled packets	*page 13-7*
dhcp-offer-convert	Enables the conversion of broadcast DHCP offers to unicast	*page 13-8*
dns-snoop	Sets the timeout value for DNS entries	*page 13-9*
firewall	Configures the wireless firewall	*page 13-10*
flow	Defines a session flow timeout	*page 13-11*
ip	Configures *Internet Protocol* (IP) components on this firewall policy	*page 13-13*
ip-mac	Defines an action based on IP-MAC table	*page 13-20*
ipv6	Configures IPv6 components on this firewall policy	*page 13-22*
ipv6-mac	Defines an action based on IPv6-MAC table	*page 13-26*
logging	Enables enhanced firewall logging	*page 13-28*
no	Negates a command or reverts settings to their default	*page 13-30*
proxy-arp	Enables the generation of ARP responses on behalf of another device	*page 13-32*
proxy-nd	Enables the generation of ND responses (for IPv6) on behalf of another device	*page 13-33*
stateful-packet-inspection-l2	Enables stateful packets-inspection in layer 2 firewall	*page 13-34*
storm-control	Defines storm control and logging settings	*page 13-35*
virtual-defragmentation	Enables virtual defragmentation of IPv4 packets	*page 13-37*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

13.1.1 acl-logging

firewall-policy

Enables logging on flow creating traffic. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
acl-logging
```

Parameters

None

Example

```
rfs4000-229D58(config-fw-policy-test)#acl-logging

rfs4000-229D58(config-fw-policy-test)#no acl-logging

rfs4000-229D58(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 no acl-logging
rfs4000-229D58(config-fw-policy-test)#
```

Related Commands

no	Disables logging on flow creating traffic

13.1.2 alg

firewall-policy

Enables traffic filtering at the application layer using the *Application Layer Gateway* (ALG) feature

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
alg [dns|facetime|ftp|pptp|sccp|sip|tftp]
```

Parameters

- `alg [dns|facetime|ftp|pptp|sccp|sip|tftp]`

alg	Enables traffic filtering at the application layer. The ALG provides filters for the following common protocols: DNS, Facetime, FTP, PPTP, SCCP, SIP, and TFTP.
dns	Allows *Domain Name System* (DNS) traffic through the firewall using its default ports. This option is enabled by default. When enabled, you can easily permit or deny traffic based on a packet's DNS name, instead of the IP address. Use this option when configuring ACLs allowing or denying traffic for Web sites that have a single domain name resolving to any one of multiple IP addresses.
facetime	Allows Apple's FaceTime video calling traffic through the firewall using its default ports. This option is disabled by default.
ftp	Allows *File Transfer Protocol* (FTP) traffic through the firewall using its default ports. This option is enabled by default.
pptp	Allows *Point-to-Point Tunneling Protocol* (PPTP) traffic through the firewall using its default ports. PPTP, a network protocol, enables secure transfer of data from a remote client to an enterprise server by encapsulating PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. This option is enabled by default
sccp	Allows *Signalling Connection Control Part* (SCCP) traffic through the firewall using its default ports. This option is disabled by default. SCCP is a network protocol that provides routing, flow control and error correction in telecommunication networks.
sip	Allows *Session Initiation Protocol* (SIP) traffic through the firewall using its default ports. This option is enabled by default.
tftp	Enables the *Trivial File Transfer Protocol* (TFTP) algorithm. When enabled, allows TFTP traffic through the firewall using its default ports. This option is enabled by default.

Example

```
nx4500-5CFA2B(config-fw-policy-test)#alg facetime

nx4500-5CFA2B(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 alg facetime
nx4500-5CFA2B(config-fw-policy-test)#
```

Related Commands

no	Removes or reverts ALG related settings

13.1.3 clamp

firewall-policy

This option limits the TCP *Maximum Segment Size* (MSS) to the size of the *Maximum Transmission Unit* (MTU) discovered by path MTU discovery for the inner protocol. This ensures the packet traverses through the inner protocol without fragmentation. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
clamp tcp-mss
```

Parameters

- `clamp tcp-mss`

tcp-mss	Limits the TCP MSS size to the MTU value of the inner protocol for tunneled packets

Example

```
rfs6000-37FABE(config-fw-policy-test)#clamp tcp-mss
```

Related Commands

no	Disables limiting of the TCP MSS

13.1.4 dhcp-offer-convert

firewall-policy

Enables the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dhcp-offer-convert
```

Parameters

None

Example

```
rfs6000-37FABE(config-fw-policy-test)#dhcp-offer-convert

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 dhcp-offer-convert
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Disables the conversion of broadcast DHCP offers to unicast

13.1.5 dns-snoop

firewall-policy

Sets the timeout interval for DNS snoop table entries. DNS snoop entries provide information, such as client to IP address and client to default gateway(s) mappings. This information is used to detect if the client is sending routed packets to a wrong MAC address.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dns-snoop entry-timeout <30-86400>
```

Parameters

- `dns-snoop entry-timeout <30-86400>`

entry-timeout <30-86400>	Sets the DNS snoop table entry timeout interval from 30 - 86400 seconds. An entry is retained in the DNS snoop table only for the specified time, and is deleted once this time is exceeded. The default is 1,800 seconds.

Example

```
rfs6000-37FABE(config-fw-policy-test)#dns-snoop entry-timeout 35

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Removes the DNS snoop table entry timeout interval

13.1.6 firewall

firewall-policy

Enables a device's firewall

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
firewall enable
```

Parameters

- `firewall enable`

firewall enable	Enables wireless firewalls

Example

```
rfs6000-37FABE(config-fw-policy-default)#firewall enable
rfs6000-37FABE(config-fw-policy-default)#
```

Related Commands

no	Disables a device's firewall

13.1.7 flow

firewall-policy

Defines the session flow timeout interval for different packet types

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
flow [dhcp|timeout]

flow dhcp stateful

flow timeout [icmp|other|tcp|udp]

flow timeout [icmp|other] <1-32400>

flow timeout udp <15-32400>

flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|stateless-
general] <1-32400>

flow timeout tcp established <15-32400>
```

Parameters

- `flow dhcp stateful`

dhcp	Configures DHCP packet flow
stateful	Performs a stateful check on DHCP packets. This feature is enabled by default.

- `flow timeout [icmp|other] <1-32400>`

timeout	Configures a packet timeout
icmp	Configures the timeout for ICMP packets. The default is 30 seconds.
other	Configures the timeout for packets other than ICMP, TCP, or UDP. The default is 30 seconds.
<1-32400>	Configures the timeout from 1 - 32400 seconds

- `flow timeout udp <15-32400>`

timeout	Configures a packet timeout
udp	Configures the timeout for UDP packets. The default is 30 seconds.
<15-32400>	Configures the timeout from 15 - 32400 seconds

- `flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|stateless-general] <1-32400>`

timeout	Configures a packet timeout
tcp	Configures the timeout for TCP packets
close-wait	Configures the closed TCP flow timeout. The default is 10 seconds.
reset	Configures the reset TCP flow timeout. The default is 10 seconds.

setup	Configures the opening TCP flow timeout. The default is 10 seconds.
stateless-fin-or-reset	Configures stateless TCP flow timeout created with the FIN or RESET packets. The default is 10 seconds.
stateless-general	Configures the stateless TCP flow timeout. The default is 90 seconds (1m 30 s).
<1-32400>	Configures the timeout from 1 - 32400 seconds

- `flow timeout tcp established <15-32400>`

timeout	Configures the packet timeout
tcp	Configures the timeout for TCP packets
established	Configures the established TCP flow timeout. The default is 5400 seconds.
<15-32400>	Configures the timeout from 15 - 32400 seconds

Example

```
rfs6000-37FABE(config-rw-policy-test)#flow timeout udp 10000
rfs6000-37FABE(config-rw-policy-test)#flow timeout icmp 16000
rfs6000-37FABE(config-rw-policy-test)#flow timeout other 16000
rfs6000-37FABE(config-rw-policy-test)#flow timeout tcp established 1500

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Removes session timeout intervals configured for different packet types

13.1.8 ip

firewall-policy

Configures *Internet Protocol* (IP) components

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip [dos|tcp]

ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-
protocol|ip-ttl-zero|ipspoof|land|option-route|router-advt|router-solicit|
smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-max-incomplete|
tcp-null-scan|tcp-post-syn|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|
twinge|udp-short-hdr|winnuke}

ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-
protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|
smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|
tcp-post-scan|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|
udp-short-hdr|winnuke} [log-and-drop|log-only] log-level [<0-7>|alerts|critical|
debugging|emergencies|errors|informational|notifications|warnings]

ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-
protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|
smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|
tcp-post-scan|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-
short-hdr|winnuke} [drop-only]

ip dos tcp-max-incomplete [high|low] <1-1000>

ip tcp [adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-
syn|validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]

ip tcp adjust-mss <472-1460>

ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn|validate-
icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]
```

Parameters

```
• ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-
protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|
smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-
scan|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|
winnuke} [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

dos	Identifies IP events as DoS events
ascend	Optional. Detects ASCEND DoS attacks Ascend DoS attacks target known vulnerabilities in various versions of Ascend routers. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.

broadcast-multicast-icmp	Optional. Detects broadcast or multicast ICMP Dos attacks Broadcast or multicast ICMP DoS attacks take advantage of ICMP behavior in response to echo replies. These attacks spoof the source address of the target and send ICMP broadcast or multicast echo requests to the rest of the network, flooding the target machine with replies.
chargen	Optional. Detects Chargen attacks The Character Generation Protocol (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements. The Chargen attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services.
fraggle	Optional. Detects Fraggle DoS attacks The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic.
ftp-bounce	Optional. Detects FTP bounce attacks A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client.
invalid-protocol	Optional. Enables a check for an invalid protocol number Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack.
ip-ttl-zero	Optional. Enables a check for the TCP/IP TTL field having a value of zero (0) The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a *Time to Live* (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload.
ipsproof	Optional. Enables a check for the IP spoofing DoS attacks IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker.
land	Optional. Detects LAND DoS attacks A *Local Area Network Denial* (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.
option-route	Optional. Enables an IP Option Record Route DoS check

router-advt	Optional. Detects router-advertisement attacks This attack uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a man-in-the-middle situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).
router-solicit	Optional. Detects router solicitation attacks The ICMP router solicitation scan is used to actively find routers on a network. A hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests
smurf	Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.
snork	Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.
tcp-bad-sequence	Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TCP connection
tcp-fin-scan	Optional. Detects TCP FIN scan attacks Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the *Finish* (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply.

tcp-intercept	Optional. Prevents TCP intercept attacks by using TCP SYN cookies A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing e-mail, using FTP service, and so on. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP *synchronization* (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests. When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.
tcp-null-scan	Optional. Detects TCP NULL scan attacks Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.
tcp-post-syn	Optional. Detects TCP post SYN DoS attacks A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an *Intrusion Detection System* (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS.
tcp-sequence-past-window	Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.
tcp-xmas-scan	Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.
tcphdrfrag	Optional. A DoS attack where the TCP header spans IP fragments
twinge	Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system

udp-short-hdr	Optional. Enables the identification of truncated UDP headers and UDP header length fields
winnuke	Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT. The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and results in high CPU utilization on the target machine.
log-and-drop	Logs the event and drops the packet
log-only	Logs the event only, the packet is not dropped
log-level	Configures the log level
<0-7>	Sets the numeric logging level
emergencies	Numerical severity 0. System is unusable
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
errors	Numerical severity 3. Indicates an error condition
warnings	Numerical severity 4. Indicates a warning condition
notification	Numerical severity 5. Indicates a normal but significant condition
informational	Numerical severity 6. Indicates a informational condition
debugging	Numerical severity 7. Debugging messages

- `ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-scan|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|winnuke} [drop-only]`

dos	Identifies IP events as DoS events
ascend	Optional. Enables an ASCEND DoS check. Ascend routers listen on UDP port 9 for packets from Ascend's Java Configurator. Sending a formatted packet to this port can cause an Ascend router to crash.
broacast-multicast-icmp	Optional. Detects broadcast or multicast ICMP packets as an attack
chargen	Optional. The *Character Generation Protocol* (chargen) is an IP suite service primarily used for testing and debugging networks. It is also used as a source of generic payload for bandwidth and QoS measurements.
fraggle	Optional. A Fraggle DoS attack checks for UDP packets to or from port 7 or 19
ftp-bounce	Optional. A FTP bounce attack is a MIM attack that enables an attacker to open a port on a different machine using FTP. FTP requires that when a connection is requested by a client on the FTP port (21), another connection must open between the server and the client. To confirm, the PORT command has the client specify an arbitrary destination machine and port for the data connection. This is exploited by the attacker to gain access to a device that may not be the originating client.
invalid-protocol	Optional. Enables a check for invalid protocol number
ip-ttl-zero	Optional. Enables a check for the TCP/IP TTL field having a value of zero (0)
ipsproof	Optional. Enables a check for IP spoofing DoS attack

land	Optional. A *Local Area Network Denial* (LAND) is a DoS attack where IP packets are spoofed and sent to a device where the source IP and destination IP of the packet are the target device's IP, and similarly, the source port and destination port are open ports on the same device. This causes the attacked device to reply to itself continuously.
option-route	Optional. Enables an IP Option Record Route DoS check
router-advt	Optional. This is an attack, where a default route entry is added remotely to a device. This route entry is given preference, and thereby exposes an attack vector.
router-solicit	Optional. Router solicitation messages are sent to locate routers as a form of network scanning. This information can then be used to attack a device.
smurf	Optional. In this attack, a large number of ICMP echo packets are sent with a spoofed source address. This causes the device with the spoofed source address to be flooded with a large number of replies.
snork	Optional. This attack causes a remote Windows™ NT to consume 100% of the CPU's resources. This attack uses a UDP packtet with a destination port of 135 and a source port of 7, 9, or 135. This attack can also be exploited as a bandwidth consuming attack.
tcp-bad-sequence	Optional. A DoS attack that uses a specially crafted TCP packet to cause the targeted device to drop all subsequent network traffic for a specific TCP connection
tcp-fin-scan	Optional. A FIN scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.
tcp-intercept	Optional. Prevents TCP intercept attacks by using TCP SYN cookies
tcp-null-scan	Optional. A TCP null scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports
tcp-post-syn	Optional. Enables a TCP post SYN DoS attack
tcp-sequence-past-window	Optional. Enables a TCP SEQUENCE PAST WINDOW DoS attack check. Disable this check to work around a bug in Windows XP's TCP stack which sends data past the window when conducting a selective ACK.
tcp-xmas-scan	Optional. A TCP XMAS scan finds services on ports. A closed port returns a RST. This allows the attacker to identify open ports.
tcphdrfrag	Optional. A DoS attack where the TCP header spans IP fragments
twinge	Optional. A twinge attack is a flood of false ICMP packets to try and slow down a system
udp-short-hdr	Optional. Enables the identification of truncated UDP headers and UDP header length fields
winnuke	Optional. This DoS attack is specific to Windows™ 95 and Windows™ NT, causing devices to crash with a blue screen
drop-only	Optional. Drops a packet without logging

- `ip dos tcp-max-incomplete [high|low] <1-1000>`

dos	Identifies IP events as DoS events
tcp-max-incomplete	Sets the limits for the maximum number of incomplete TCP connections
high	Sets the upper limit for the maximum number of incomplete TCP connections
low	Sets the lower limit for the maximum number of incomplete TCP connections
<1-1000>	Sets the range limit from 1 - 1000 connections

- `ip tcp adjust-mss <472-1460>`

tcp	Identifies and configures TCP events and configuration items
adjust-mss	Adjusts the TCP *Maximum Segment Size* (MSS). Use this option to adjust the MSS for TCP segments on the router.
<472-1460>	Sets the TCP MSS value from 472 - 1460 bytes. The default is 472 bytes.

- `ip tcp [optimize-unnecessary-resends|recreate-flow-on-out-of-state-syn| validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]`

tcp	Identifies and configures TCP events and configuration items
optimize-unnecessary-resends	Enables the validation of unnecessary TCP packets
recreate-flow-on-out-of-state-sync	Allows a TCP SYN packet to delete an old flow in TCP_FIN_FIN_STATE, and TCP_CLOSED_STATE states and create a new flow
validate-icmp-unreachable	Enables the validation of the sequence number in ICMP unreachable error packets, which abort an established TCP flow
validate-rst-ack-number	Enables the validation of the acknowledgment number in RST packets, which abort a TCP flow
validate-rst-seq-number	Enables the validation of the sequence number in RST packets, which abort an established TCP flow

Example

```
rfs6000-37FABE(config-rw-policy-test)#ip dos fraggle drop-only
rfs6000-37FABE(config-rw-policy-test)#ip dos tcp-max-incomplete high 600
rfs6000-37FABE(config-rw-policy-test)#ip dos tcp-max-incomplete low 60
rfs6000-37FABE(config-fw-policy-test)#ip dos tcp-sequence-past-window drop-only

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Resets firewall policy IP components

13.1.9 ip-mac

firewall-policy

Defines an action based on the device IP MAC table, and also detects conflicts between IP addresses and MAC addresses

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ip-mac [conflict|routing]

ip-mac conflict drop-only

ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]

ip-mac routing conflict drop-only

ip-mac routing [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|
emergencies|errors|informational|notifications|warnings]
```

Parameters

- `ip-mac conflict drop-only`

conflict	Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default.
drop-only	Drops a packet without logging

- `ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|alerts|critical| debug|emergencies|errors|informational|notifications|warnings]`

conflict	Action performed when a conflict exists between the IP address and MAC address. This option is enabled by default.
log-and-drop	Logs the event and drops the packet. This is the default setting.
log-only	Logs the event only, the packet is not dropped
log-level	Configures the log level
<0-7>	Sets the numeric logging level
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
debugging	Numerical severity 7. Debugging messages
emergencies	Numerical severity 0. System is unusable
errors	Numerical severity 3. Indicates an error condition
informational	Numerical severity 6. Indicates a informational condition
notification	Numerical severity 5. Indicates a normal but significant condition
warnings	Numerical severity 4. Indicates a warning condition. This is the default setting

- `ip-mac routing conflict drop-only`

routing	Enables IPMAC routing conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address.
conflict	Defines the action performed when a routing table conflict is detected. This option is enabled by default.
drop-only	Drops a packet without logging

- `ip-mac routing [log-and-drop|log-only] log-level [<0-7>|alerts|critical|debug|emergencies|errors|informational|notifications|warnings]`

routing	Defines a routing table based action
conflict	Action performed when a conflict exists in the routing table. This option is enabled by default.
log-and-drop	Logs the event and drops the packet. This is the default setting.
log-only	Logs the event only, the packet is not dropped
log-level	Configures the log level to log this event under
<0-7>	Sets the numeric logging level
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
debugging	Numerical severity 7. Debugging messages
emergencies	Numerical severity 0. System is unusable
errors	Numerical severity 3. Indicates an error condition
informational	Numerical severity 6. Indicates a informational condition
notification	Numerical severity 5. Indicates a normal but significant condition
warnings	Numerical severity 4. Indicates a warning condition. This is the default setting.

Example

```
rfs6000-37FABE(config-rw-policy-test)#ip-mac conflict drop-only
rfs6000-37FABE(config-rw-policy-test)#ip-mac routing conflict log-and-drop log-
level notifications

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-only log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Disables actions based on device IP MAC table, IP address, and MAC address conflict detection

13.1.10 ipv6

firewall-policy

Configures IPv6 components on this firewall policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 [dos|duplicate-options|firewall|option|rewrite-flow-label|routing-type|
strict-ext-hdr-check|unknown-options]

ipv6 dos {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility} [drop-only|
log-and-drop|log-only]

ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-
options] [drop-only|log-and-drop|log-only]

ipv6 option {endpoint-identification|network-service-access-point|router-alert|
strict-hao-opt-alert|strict-padding} [drop-only|log-and-drop|log-only]

ipv6 [firewall enable|rewrite-flow-label]
```

Parameters

```
• ipv6 dos {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility} [drop-
only|log-and-drop|log-only]
```

dos	Identifies IPv6 events as DoS events
hop-limit-zero	Optional. Enables checking of IPv6 hop limit field. If the IPv6 hop limit field is ZERO (0) it is considered as attack. This option is enabled by default.
multicast-icmpv6	Optional. Enables detection of multicast ICMPv6 traffic as attack. This option is applicable only to ICMPv6 Echo request or reply packets. This option is enabled by default.
tcp-intercept-mobility	Optional. Enables detection of IPv6 TCP packets with mobility option "HAO(Home-Address-Option)" or "RH(Routing Header) type two". When enabled, this option also detects the “don't generate TCP syn cookies” for such packets. This option is enabled by default.
drop-only	This parameter is common to all of the above keywords. Drops all packets. Drops the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility).
log-and-drop	Logs the event and drops the packet. Drops the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility) and logs an event.
log-only	Logs the event only, the packet is not dropped. Does not drop the specified packet type (hop-limit-zero, multicast-icmpv6, and tcp-intercept-mobility). But, an event is logged.

log-level	If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: • <0-7> – Sets the numeric logging level • alerts – Numerical severity 1. Indicates a condition where immediate action is required • critical – Numerical severity 2. Indicates a critical condition • debugging – Numerical severity 7. Debugging messages • emergencies – Numerical severity 0. System is unusable • errors – Numerical severity 3. Indicates an error condition • informational – Numerical severity 6. Indicates a informational condition • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

- `ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check| unknown-options] [drop-only|log-and-drop|log-only]`

duplicate-options	Enables handling of duplicate options in hop-by-hop and destination option extension headers. This configuration excludes HAO handling. This option is enabled by default.
routing-type [one|two]	Enables checking of the following IPv6 routing types: • one – Routing Type 1(Nimrod routing). This option is disabled by default. • two – Routing Type 2(Mobile IP). This option is disabled by default.
strict-ext-hdr-check	Enables strict checking for out of order and number of occurrences of extension header. This option is enabled by default.
unknown-options	Enables handling unknown options in hop-by-hop and destination option extension headers. This option is enabled by default.
drop-only	This parameter is common to all of the above keywords. Drops all packets. Drops the packet if matching any of the above specified types.
log-and-drop	Logs the event and drops the packet. Drops the packet, if matching any of the above specified types, and logs an event.
log-only	Logs the event only, the packet is not dropped. Does not drop the packet, if matching any of the above specified types. But an event is logged.
log-level	If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: • <0-7> – Sets the numeric logging level • alerts – Numerical severity 1. Indicates a condition where immediate action is required • critical – Numerical severity 2. Indicates a critical condition • debugging – Numerical severity 7. Debugging messages • emergencies – Numerical severity 0. System is unusable • errors – Numerical severity 3. Indicates an error condition • informational – Numerical severity 6. Indicates a informational condition • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

- `ipv6 option {endpoint-identification|network-service-access-point|router-alert|strict-hao-opt-alert|strict-padding} [drop-only|log-and-drop|log-only]`

option	Enables checking for the following ipv6 extension header options: • End point identification option (disabled by default) • Network service access point address option (disabled by default) • Router alert option (disabled by default) • Home address option in destination option extension header (enabled by default) • Pad1 and PadN options validating (enabled by default) All of these are optional parameters. If no option is specified, the system enables checks as per the default values.
drop-only	This parameter is common to all of the above keywords. Drops all packets. Drops the packet if matching any of the above specified “option” types.
log-and-drop	Logs the event and drops the packet. Drops the packet, if matching any of the above specified “option” types, and logs an event.
log-only	Logs the event only, the packet is not dropped. Does not drop the packet, if matching any of the above specified “option” types. But an event is logged.
log-level	If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: • <0-7> – Sets the numeric logging level • alerts – Numerical severity 1. Indicates a condition where immediate action is required • critical – Numerical severity 2. Indicates a critical condition • debugging – Numerical severity 7. Debugging messages • emergencies – Numerical severity 0. System is unusable • errors – Numerical severity 3. Indicates an error condition • informational – Numerical severity 6. Indicates a informational condition • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

- `ipv6 [firewall enable|rewrite-flow-label]`

firewall enable	Enables IPv6 firewall. This option is enabled by default.
rewrite-flow-label	Rewrites the IPv6 flow label field of every packet. This option is disabled by default.

Example

```
nx4500-5CFA2B(config-fw-policy-test)#ipv6 dos hop-limit-zero drop-only

nx4500-5CFA2B(config-fw-policy-test)#ipv6 routing-type two log-and-drop log-level
warnings

nx4500-5CFA2B(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
nx4500-5CFA2B(config-fw-policy-test)#
```

Related Commands

no	Resets this firewall policy's IPv6 components

13.1.11 ipv6-mac

firewall-policy

Defines an action based on conflicts detected in a device's IPv6 and MAC addresses

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6-mac [conflict|routing]

ipv6-mac conflict [drop-only|log-and-drop|log-only]

ipv6-mac routing conflict [drop-only|log-and-drop|log-only]
```

Parameters

- `ipv6-mac conflict [drop-only|log-and-drop|log-only]`

conflict	Enables detection of conflict between a device's IPv6 and MAC addresses. This option is enabled by default. This command also specifies the action to be performed when a such a conflict is detected. The options are: drop-only, log-and-drop, and log-only
drop-only	Drops a packet (with conflicting IPv6 and MAC address) without logging
log-and-drop	Logs the event and drops the packet. This is the default setting.
log-only	Logs the event only, the packet is not dropped
log-level	If selecting the "log-and-drop" and "log-only" action type, specify the log level. The options are: • <0-7> – Sets the numeric logging level • alerts – Numerical severity 1. Indicates a condition where immediate action is required • critical – Numerical severity 2. Indicates a critical condition • debugging – Numerical severity 7. Debugging messages • emergencies – Numerical severity 0. System is unusable • errors – Numerical severity 3. Indicates an error condition • informational – Numerical severity 6. Indicates a informational condition • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

- `ipv6-mac routing conflict [drop-only|log-and-drop|log-only]`

routing conflict	Enables detection of conflict between the next-hop's IPv6 and MAC addresses. This option is enabled by default. This command also specifies the action to be performed when a such a conflict is detected. The options are: drop-only, log-and-drop, and log-only

drop-only	Drops a packet (with conflicting next-hop IPv6 and MAC addresses) without logging
log-and-drop	Logs the event and drops the packet. This is the default setting.
log-only	Logs the event only, the packet is not dropped
log-level	If selecting the “log-and-drop” and “log-only” action type, specify the log level. The options are: • <0-7> – Sets the numeric logging level • alerts – Numerical severity 1. Indicates a condition where immediate action is required • critical – Numerical severity 2. Indicates a critical condition • debugging – Numerical severity 7. Debugging messages • emergencies – Numerical severity 0. System is unusable • errors – Numerical severity 3. Indicates an error condition • informational – Numerical severity 6. Indicates a informational condition • notifications – Numerical severity 5. Indicates a normal but significant condition • warnings – Numerical severity 4. Indicates a warning condition. This is the default setting.

Example

```
nx4500-5CFA2B(config-fw-policy-test)#ipv6-mac routing conflict drop-only

nx4500-5CFA2B(config-fw-policy-test)#show context
firewall-policy test
 no ip dos tcp-sequence-past-window
 ipv6 routing-type two log-and-drop log-level warnings
 ipv6 dos hop-limit-zero drop-only
 ipv6-mac routing conflict drop-only
nx4500-5CFA2B(config-fw-policy-test)#
```

Related Commands

no	Disables actions based on device IPv6 MAC table, next-hop’s IPv6 and MAC address conflict detection

13.1.12 logging

firewall-policy

Configures enhanced firewall logging

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
logging [icmp-all|icmp-packet-drop|malformed-packet-drop|verbose]

logging icmp-all
logging verbose
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

Parameters

- `logging icmp-all`

logging	Configures enhanced firewall logging parameters
icmp-all	Enables logging of all ICMPv4/v6 packets allowed by the firewall. This option is disabled by default.

- `logging verbose`

logging	Configures enhanced firewall logging parameters. This option is disabled by default.
verbose	Enables verbose logging

- `logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]`

logging	Configures enhanced firewall logging parameters
icmp-packet-drop	Drops ICMP (ICMPv4 and ICMPv6) packets that do not pass sanity checks. The default is none.
malformed-packet-drop	Drops raw IP (IPv4 and IPv6) packets that do not pass sanity checks. The default is none.
all	Logs all messages
rate-limited	Enables rate-limited logging. This option sets the rate limit for log messages to one message every 20 seconds.

Example

```
rfs6000-37FABE(config-rw-policy-test)#logging verbose
rfs6000-37FABE(config-rw-policy-test)#logging icmp-packet-drop rate-limited
rfs6000-37FABE(config-rw-policy-test)#logging malformed-packet-drop all
rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 ip dos tcp-sequence-past-window drop-only
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 ip-mac conflict drop-only
 ip-mac routing conflict log-only log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#

nx9500-6C8809(config-fw-policy-test2)#show context
firewall-policy test2
 no ip dos tcp-sequence-past-window
nx9500-6C8809(config-fw-policy-test2)#

nx9500-6C8809(config-fw-policy-test2)#logging icmp-all

nx9500-6C8809(config-fw-policy-test2)#show context
firewall-policy test2
 no ip dos tcp-sequence-past-window
 logging icmp-all
nx9500-6C8809(config-fw-policy-test2)
```

Related Commands

no	Disables enhanced firewall logging

13.1.13 no

firewall-policy

Negates a command or sets the default for firewall policy commands

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [acl-logging|alg|clamp|dhcp-offer-convert|dns-snoop|firewall|flow|ip|ip-mac|
ipv6|ipv6-mac|logging|proxy-arp|proxy-nd|stateful-packet-inspection-l2|
storm-control|virtual-defragmentation]

no [acl-logging|dhcp-offer-convert|proxy-arp|proxy-nd|stateful-packet-inspection-
l2]

no alg [dns|facetime|ftp|pptp|sccp|sip|tftp]

no clamp tcp-mss

no dns-snoop entry-timeout

no firewall enable

no flow dhcp stateful

no flow timeout [icmp|other|udp]

no flow timeout tcp [closed-wait|established|reset|setup|stateless-fin-or-reset|
stateless-general]

no ip dos {ascend|broadcast-multicast-icmp|chargen|fraggle|ftp-bounce|invalid-
protocol|ip-ttl-zero|ipsproof|land|option-route|router-advt|router-solicit|
smurf|snork|tcp-bad-sequence|tcp-fin-scan|tcp-intercept|tcp-null-scan|tcp-post-
syn|tcp-sequence-past-window|tcp-xmas-scan|tcphdrfrag|twinge|udp-short-hdr|
winnuke}

no ip tcp [adjust-mss|optimize-unnecessary-resends|recreate-flow-on-out-of-state-
syn|validate-icmp-unreachable|validate-rst-ack-number|validate-rst-seq-number]

no ip-mac conflict

no ip-mac routing conflict

no ipv6 [dos|duplicate-options|firewall|option|rewrite-flow-label|routing-type|
strict-ext-hdr-check|unknown-options]

no ipv6 dos {hop-limit-zero|multicast-icmpv6|tcp-intercept-mobility}

no ipv6 [duplicate-options|routing-type [one|two]|strict-ext-hdr-check|unknown-
options]

no ipv6 option {endpoint-identification|network-service-access-point|router-
alert|strict-hao-opt-alert|strict-padding}

no ipv6 [firewall enable|rewrite-flow-label]

no logging [icmp-all|icmp-packet-drop|verbose|malformed-packet-drop]
```

```
no storm-control [arp|broadcast|multicast|unicast] {fe <1-4>|ge <1-8>|log|port-
channel <1-8>|up1|wlan <WLAN-NAME>}

no virtual-defragmentation {maximum-fragments-per-datagram|minimum-first-
fragment-length|maximum-defragmentation-per-host|timeout}
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates a command or sets the default for firewall policy commands.

Example

```
rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 no ip dos tcp-sequence-past-window
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log warnings
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#

rfs6000-37FABE(config-fw-policy-test)#no ip dos fraggle
rfs6000-37FABE(config-fw-policy-test)#no storm-control arp log
rfs6000-37FABE(config-fw-policy-test)#no dhcp-offer-convert
rfs6000-37FABE(config-fw-policy-test)#no logging malformed-packet-drop

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 no ip dos fraggle
 no ip dos tcp-sequence-past-window
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log none
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 logging icmp-packet-drop rate-limited
 logging verbose
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#
```

13.1.14 proxy-arp

firewall-policy

Enables the generation of ARP responses on behalf of another device. Proxy ARP allows the Firewall to handle ARP routing requests for devices behind the firewall. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
proxy-arp
```

Parameters

None

Example

```
rfs6000-37FABE(config-fw-policy-test)#proxy-arp
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Disables the generation of ARP responses on behalf of another device

13.1.15 proxy-nd

firewall-policy

Enables generation of ND responses (for IPv6) on behalf of another device

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
proxy-nd
```

Parameters

None

Example

```
nx9500-6C8809(config-fw-policy-fw1)#proxy-nd
nx9500-6C8809(config-fw-policy-fw1)#
```

Related Commands

no	Disables the generation of ND responses on behalf of another device

13.1.16 stateful-packet-inspection-12

firewall-policy

Enables layer 2 firewall stateful packet inspection. When enabled, allows stateful packet inspection for RF Domain manager routed interfaces within the layer 2 firewall. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
stateful-packet-inspection-l2
```

Parameters

None

Example

```
rfs6000-37FABE(config-fw-policy-test)#stateful-packet-inspection-l2
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Disables stateful packet inspection in a layer 2 firewall

13.1.17 storm-control

firewall-policy

Enables storm control on the firewall policy

Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the RF Domain manager interface.

Storm control limits multicast, unicast and broadcast frames accepted and forwarded by a device. Messages are logged based on their severity level.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
storm-control [arp|broadcast|multicast|unicast]
storm-control [arp|broadcast|multicast|unicast] [level|log]

storm-control [arp|broadcast|multicast|unicast] level <1-1000000> [fe <1-4>|ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]

storm-control [arp|broadcast|multicast|unicast] log [<0-7>|alerts|critical|debugging|emergencies|errors|informational|none|notifications|warnings]
```

Parameters

```
• storm-control [arp|broadcast|multicast|unicast] level <1-1000000> [fe <1-4>|ge <1-8>|port-channel <1-8>|up1|wlan <WLAN-NAME>]
```

arp	Configures storm control for ARP packets
broadcast	Configures storm control for broadcast packets
multicast	Configures storm control for multicast packets
unicast	Configures storm control for unicast packets
level <1-1000000>	Configures the allowed number of packets received per second before storm control begins • <1-1000000> – Sets the number of packets received per second
fe <1-4>	Sets the FastEthernet port for storm control from 1 - 4
ge <1-8>	Sets the GigabitEthernet port for storm control from 1 - 8
port-channel <1-8>	Sets the port channel for storm control from 1- 8
up1	Sets the uplink interface
wlan <WLAN-NAME>	Configures the WLAN • <WLAN-NAME> – Sets the WLAN ID for the storm control configuration

```
• storm-control [arp|bcast|multicast|unicast] log [<0-7>|alerts|critical|
debugging|emergencies|errors|informational|none|notifications|warnings]
```

arp	Configures storm control for ARP packets
broadcast	Configures storm control for broadcast packets
multicast	Configures storm control for multicast packets
unicast	Configures storm control for unicast packets
log	Configures the storm control log level for storm control events
<0-7>	Sets the numeric logging level from 0 - 7
alerts	Numerical severity 1. Indicates a condition where immediate action is required
critical	Numerical severity 2. Indicates a critical condition
debugging	Numerical severity 7. Debugging messages
emergencies	Numerical severity 0. System is unusable
errors	Numerical severity 3. Indicates an error condition
informational	Numerical severity 6. Indicates a informational condition
none	Disables storm control logging
notification	Numerical severity 5. Indicates a normal but significant condition
warnings	Numerical severity 4. Indicates a warning condition. This is the default setting.

Example

```
rfs6000-37FABE(config-fw-policy-test)#storm-control arp log warning

rfs6000-37FABE(config-fw-policy-test)#storm-control broadcast level 20000 ge 4

rfs6000-37FABE(config-fw-policy-test)#show context
firewall-policy test
 ip dos fraggle drop-only
 no ip dos tcp-sequence-past-window
 ip dos tcp-max-incomplete high 600
 ip dos tcp-max-incomplete low 60
 storm-control broadcast level 20000 ge 4
 storm-control arp log warnings
 ip-mac conflict drop-only
 ip-mac routing conflict log-and-drop log-level notifications
 flow timeout icmp 16000
 flow timeout udp 10000
 flow timeout tcp established 1500
 flow timeout other 16000
 dhcp-offer-convert
 logging icmp-packet-drop rate-limited
 logging malformed-packet-drop all
 logging verbose
 dns-snoop entry-timeout 35
rfs6000-37FABE(config-fw-policy-test)#
```

Related Commands

no	Disables storm control limits on multicast, unicast, and broadcast frames accepted and forwarded by a device

13.1.18 virtual-defragmentation

firewall-policy

Enables the virtual de-fragmentation of IPv4 and IPv6 packets. This parameter is required for optimal firewall functionality and is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|maximum-
fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>|timeout
<1-60>}
```

Parameters

```
• virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|maximum-
fragments-per-datagram <2-8129>|minimum-first-fragment-length <8-1500>|timeout
<1-60>}
```

maximum-defragmentation-per-host <1-16384>	Optional. Configures the maximum number of active defragmentations allowed per host before it is dropped (applicable to IPv4 and IPV6 packets) • <1-16384> – Sets a value from 1 - 16384. The default is 8.
maximum-fragments-per-datagram <2-8129>	Optional. Configures the maximum number of fragments allowed in a datagram before it is dropped (applicable to IPv4 and IPV6 packets) • <2-8129> – Sets a value from 2 - 8129. The default is 140.
minimum-first-fragment-length <8-1500>	Optional. Defines the minimum length required for the first fragment (applicable to IPv4 and IPV6 packets) • <8-1500> – Sets a value from 8 - 1500 bytes. The default is 8 bytes.
timeout <1-60>	Optional. Configures a virtual defragmentation timeout, in seconds, applicable to both IPv4 and IPv6 packets • <1-60> – Specify a value from 1 - 60 seconds. The default is 1 second.

Example

```
rfs6000-37FABE(config-fw-policy-test)#virtual-defragmentation maximum-fragments-
per-datagram 10
rfs6000-37FABE(config-fw-policy-test)#virtual-defragmentation minimum-first-
fragment-length 100
```

Related Commands

no	Resets values or disables virtual defragmentation settings

14 MINT-POLICY

This chapter summarizes MiNT policy commands in the CLI command structure.

All communication using the MiNT transport layer can be optionally secured. This includes confidentiality, integrity and authentication of all communications. In addition, a device can be configured to communicate over MiNT with other devices authorized by an administrator.

Use the (config) instance to configure mint-policy related configuration commands. To navigate to the config MiNT policy instance, use the following command:

```
<DEVICE>(config)#mint-policy global-default

rfs6000-37FABE(config-mint-policy-global-default)#?
Mint Policy Mode commands:
  level    Mint routing level
  lsp      LSP
  mtu      Configure the global Mint MTU
  no       Negate a command or set its defaults
  router   Mint router
  udp      Configure mint UDP/IP encapsulation

  clrscr   Clears the display screen
  commit   Commit all changes made in this session
  do       Run commands from Exec mode
  end      End current mode and change to EXEC mode
  exit     End current mode and down to previous mode
  help     Description of the interactive help system
  revert   Revert changes
  service  Service Commands
  show     Show running system information
  write    Write running configuration to memory or terminal

rfs6000-37FABE(config-mint-policy-global-default)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

14.1 mint-policy

- *MINT-POLICY*

The following table summarizes MiNT policy configuration commands:

Table 14.1 *MiNT-Policy-Config Commands*

Command	Description	Reference
level	Configures the MiNT routing level	*page 14-3*
lsp	Enables adding of checksum to LSP messages forwarded across MiNT links	*page 14-4*
mtu	Configures the global MiNT MTU	*page 14-5*
no	Negates a command or sets its default	*page 14-8*
router	Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)	*page 14-6*
udp	Configures the MiNT UDP/IP encapsulation parameters	*page 14-7*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

14.1.1 level

mint-policy

Configures the global MiNT routing level

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
level 2 area-id <1-16777215>
```

Parameters

- `level 2 area-id <1-16777215>`

level 2	Configures level 2 inter-site MiNT routing
area-id <1-16777215>	Configures the routing area identifier • <1-16777215> – Specify a value from 1 - 16777215. The level 2 area ID is the global MiNT area identifier. This area identifier separates two overlapping MiNT networks. Configure the level 2 area ID only if there are two MiNT networks sharing the same packet broadcast domain.

Example

```
rfs6000-37FABE(config-mint-policy-global-default)#level 2 area-id 2000

rfs6000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 level 2 area-id 2000
rfs6000-37FABE(config-mint-policy-global-default)#
```

Related Commands

no	Disables level 2 MiNT packet routing (inter-site packet routing)

14.1.2 lsp

mint-policy

Enables adding of checksum to *label-switched path* (LSP) messages forwarded across MiNT links. When enabled, this option helps to verify integrity of LSP messages. LSP messages exchanged over MiNT links are often corrupted. These LSP corruptions cause inaccuracies in the *Shortest Path First* (SPF) calculation process, leading to access point adoption related issues. Enabling LSP checksum helps troubleshooting adoption-related issues.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
lsp checksum
```

Parameters

- `lsp checksum`

lsp checksum	Enables adding of checksum to LSP messages forwarded across MiNT links. When enabled, the integrity of LSP messages is verified by matching the LSP message checksum at the MiNT link end nodes. In case of a match the message is uncorrupted.

Example

```
nx4500-5CFA2B(config-mint-policy-global-default)#lsp checksum

nx4500-5CFA2B(config-mint-policy-global-default)#show context
mint-policy global-default
 lsp checksum
nx4500-5CFA2B(config-mint-policy-global-default)#
```

Related Commands

no	Disables adding of checksum to LSP messages forwarded across MiNT links

14.1.3 mtu

mint-policy

Configures global MiNT *Multiple Transmission Unit* (MTU). Use this command to specify the maximum packet size, in bytes, for MiNT routing. Higher the MTU values, greater is the network efficiency. The user data per packet increases, while protocol overheads, such as headers or underlying per-packet delays remain the same.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mtu <900-1500>
```

Parameters

- `mtu <900-1500>`

<900-1500>	Specifies the maximum packet size from 900 - 1500 bytes The maximum packet size specified is rounded down to a value using the following formula: 4 + a multiple of 8. The MTU setting specifies the maximum packet size used for MiNT packets. Larger packets are fragmented to fit within the specified packet size limit. You may want to configure this parameter if the MiNT backhaul network requires or recommends smaller packet sizes. The default value is 1500 bytes.

Example

```
rfs6000-37FABE(config-mint-policy-global-default)#mtu 1000

rfs6000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 mtu 996
 level 2 area-id 2
rfs6000-37FABE(config-mint-policy-global-default)#
```

Related Commands

no	Reverts the configured MiNT MTU value to its default (1500 bytes) Negates the configured maximum packet size for MiNT routing

14.1.4 router

mint-policy

Configures the priority for MiNT router packets (HELLO, LSP, PSNP, and EXTVLAN)

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
router packet priority <0-7>
```

Parameters

- `router packet priority <0-7>`

router packet priority <0-7>	Allows you to configure the priority for MiNT router packets from 0 - 7. The default is 5. Higher the value higher is the priority. Therefore, seven (7) represents highest priority.

Example

```
rfs4000-229D58(config-mint-policy-global-default)#router packet priority 4

rfs4000-229D58(config-mint-policy-global-default)#show context
mint-policy global-default
 router packet priority 4
rfs4000-229D58(config-mint-policy-global-default)#
```

Related Commands

no	Reverts the MiNT router packet priority to default (5)

14.1.5 udp

mint-policy

Configures MiNT UDP/IP encapsulation parameters. Use this command to configure the default UDP port used for MiNT control packet encapsulation.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
udp port <2-65534>
```

Parameters

- `udp port <2-65534>`

port <2-65534>	Configures default UDP port used for MiNT control packet encapsulation • <2-65534> – Enter a value from 2 - 65534. This value specifies an alternate UDP port used by MiNT control packets and must be an even number. The specified port number plus 1 is used to carry MiNT data packets. The default value is 24576.

Example

```
rfs6000-37FABE(config-mint-policy-global-default)#udp port 1024

rfs6000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 udp port 1024
 mtu 996
 level 2 area-id 2000
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
rfs6000-37FABE(config-mint-policy-global-default)#
```

Related Commands

no	Reverts MiNT UDP/IP encapsulation to its default

14.1.6 no

mint-policy

Negates a command or reverts values to their default. When used in the config MiNT policy mode, the `no` command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [level|lsp|mtu|router|udp]

no level 2 area-id

no lsp checksum

no mtu

no router packet priority

no udp port <LINE-SINK>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	The `no` command resets or reverts the following global MiNT policy parameters: routing level, MTU, router packet priority, and UDP or IP encapsulation settings.

Example

The following example shows the global Mint Policy parameters before the 'no' commands are executed:

```
rfs6000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 udp port 1024
 mtu 996
 level 2 area-id 2000
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
rfs6000-37FABE(config-mint-policy-global-default)#

rfs6000-37FABE(config-mint-policy-global-default)#no level 2 area-id
rfs6000-37FABE(config-mint-policy-global-default)#no mtu
rfs6000-37FABE(config-mint-policy-global-default)#no udp port
```

The following example shows the global Mint Policy parameters after the 'no' commands are executed:

```
rfs6000-37FABE(config-mint-policy-global-default)#show context
mint-policy global-default
 sign-unknown-device
 security-level control-and-data
 rejoin-timeout 1000
rfs6000-37FABE(config-mint-policy-global-default)#
```

15 MANAGEMENT-POLICY

This chapter summarizes management policy commands in the CLI command structure.

A management policy contains configuration elements for managing a device, such as access control, SNMP, admin user credentials, and roles.

A controller (wireless controller, access point, or service platform) uses mechanisms to allow or deny device access to separate interfaces and protocols (*HTTP, HTTPS*, *FTP*, *Telnet*, *SSH* or *SNMP*). Management access can be enabled or disabled as required for unique policies. The management access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can do the following:

- Restrict SNMP, CLI and Web UI access to specific hosts or subnets.
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.
- Provide authentication for management users.
- Apply access restrictions and permissions to management users.

Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.

Access Points utilize a single management access policy, so ensure all the intended administrative roles, permissions, authentication and SNMP settings are correctly set. If an access point is functioning as a virtual controller AP, these are the access settings used by adopted access points of the same model as the virtual controller AP.

It is recommended to disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices.

Use the (config) instance to configure a management policy. To navigate to the config management policy instance, use the following commands:

```
<DEVICE>(config)#management-policy <POLICY-NAME>
```

To commit a management-policy, the policy must have at least one admin user account configured.

```
<DEVICE>(config-management-policy-<POLICY-NAME>)#user admin password 0 test role
superuser access all
<DEVICE>(config-management-policy-<POLICY-NAME>)#

<DEVICE>(config-management-policy-<POLICY-NAME>)#?
Management Mode commands:
  aaa-login                 Set authentication for logins
  allowed-locations         Add allowed locations
  banner                    Define a login banner
  ftp                       Enable FTP server
  http                      Hyper Text Terminal Protocol (HTTP)
  https                     Secure HTTP
  idle-session-timeout      Configure idle timeout for a configuration session
                            (GUI or CLI)
  ipv6                      IPv6 Protocol
  no                        Negate a command or set its defaults
  passwd-retry              Lockout user if too many consecutive login failures
  privilege-mode-password   Set the password for entering CLI privilege mode
  rest-server               Enable rest server for device on-boarding
                            functionality
  restrict-access           Restrict management access to the device
  snmp-server               SNMP
  ssh                       Enable ssh
  t5                        T5 configuration
  telnet                    Enable telnet
  user                      Add a user account

  clrscr                     Clears the display screen
  commit                     Commit all changes made in this session
  do                        Run commands from Exec mode
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or terminal

<DEVICE>(config-management-policy-<POLICY-NAME>)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

15.1 management-policy

- *MANAGEMENT-POLICY*

The following table summarizes management policy configuration commands:

Table 15.1 *Management-Policy-Config Commands*

Command	Description	Reference
aaa-login	Configures login authentication settings	*page 15-5*
allowed-locations	Configures a user-role based access control to RF Domains and locations with respect to the NSight *user interface* (UI)	*page 15-7*
banner	Configures the *message of the day* (motd) text	*page 15-9*
ftp	Enables FTP on this management policy	*page 15-10*
http	Enables HTTP on this management policy	*page 15-12*
https	Enables HTTPS on this management policy	*page 15-13*
idle-session-timeout	Sets the interval after which an idle session is terminated	*page 15-15*
ipv6	Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively	*page 15-16*
no	Removes or resets this management policy's settings	*page 15-18*
passwd-entry	Configures user-account lockout and unlock parameters	*page 15-20*
privilege-mode-password	Configures the CLI's privilege mode access password	*page 15-22*
rest-server	Enables the *Representational State Transfer* (REST) server to facilitate device on-boarding	*page 15-24*
restrict-access	Restricts management access to a set of hosts or subnets	*page 15-25*
snmp-server	Sets the SNMP server settings on this management policy	*page 15-28*
ssh	Enables SSH on this management policy	*page 15-33*
t5	Configures SNMP server settings for T5 devices on this management policy. This command is available only RFS4000, RFS6000, and NX95XX platforms.	*page 15-34*
telnet	Enables Telnet on this management policy	*page 15-36*
user	Creates a new user account	*page 15-37*
service	Invokes service commands to troubleshoot or debug `(config-if)` instance configurations	*page 15-41*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

15.1.1 aaa-login

management-policy

Configures *Authentication, Authorization and Accounting* (AAA) authentication mode used with this management policy. The different modes are: local authentication and external RADIUS server authentication.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
aaa-login [local|radius|tacacs]

aaa-login local

aaa-login radius [external|fallback|policy]
aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]

aaa-login tacacs [accounting|authentication|authorization|fallback|policy]
aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-TACACS-POLICY-NAME>]
```

Parameters

- `aaa-login local`

local	Sets local as the preferred authentication mode. Local authentication uses the local username database to authenticate a user. **Note:** The AP6511 and AP6521 platforms do not support local RADIUS resource.

- `aaa-login radius [external|fallback|policy <AAA-POLICY-NAME>]`

radius	Configures the RADIUS server parameters **Note:** If local authentication is disabled, use this command to specify if the RADIUS server used is external, fallback, or specified by a AAA policy.
external	Configures external RADIUS server as the preferred authentication mode
fallback	Configures RADIUS server authentication as the primary authentication mode When RADIUS server authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.
policy <AAA-POLICY-NAME>	Associates a specified AAA policy with this management policy. The AAA policy determines if a client is granted access to the network. • <AAA-POLICY-NAME> – Specify the AAA policy name (should be existing and configured). **Note:** For more information on configuring AAA policy, see *AAA-POLICY*.

```
• aaa-login tacacs [accounting|authentication|authorization|fallback|policy <AAA-
TACACS-POLICY-NAME>]
```

tacacs	Configures *Terminal Access Control Access-Control System* (TACACS) server parameters
accounting	Configures TACACS accounting
authentication	Configures TACACS authentication
authorization	Configures TACACS authorization
fallback	Configures TACACS as the primary authentication mode. When TACACS authentication fails, the system uses local authentication. This command configures local authentication as a backup mode.
policy <AAA-TACACS-POLICY-NAME>	Associates a specified AAA TACACS policy with this management policy. TACACS policies control user access to devices and network resources while providing separate accounting, authentication, and authorization services. • <AAA-TACACS-POLICY-NAME> – Specify the TACACS policy name (should be existing and configured). **Note:** For more information on configuring AAA TACACS policy, see *AAA-TACACS-POLICY*.

Usage Guidelines

Use AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

Example

```
rfs6000-37FABE(config-management-policy-test)#aaa-login radius external

rfs6000-37FABE(config-management-policy-test)#aaa-login radius policy test

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 aaa-login radius external
 aaa-login radius policy test
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Removes the TACACS server settings

15.1.2 allowed-locations

management-policy

Configures a user-role based access control to RF Domains and locations with respect to the NSight *user interface* (UI). When configured, this access control is enforced only on the NSight UI. The WiNG and NSight applications may have the same users with different permissions defined in each application. Various user roles are supported in WiNG (superuser, system-admin, network-admin, security-admin, device-provisioning-admin, helpdesk and monitor). With NSight, a user logging into the NSight UI should also have an access control restriction based on the role they're assigned. For example, a WiNG user with helpdesk privileges should have access to only the site (RF Domain) in which the helpdesk is situated, and the location tree should contain only one RF Domain. Similarly, when a user responsible for a set of sites logs in NSight, their location tree needs to contain the RF Domains for which they're responsible.

NOTE: For more information on NSight-policy configuration, see *nsight-policy*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
allowed-locations <WORD> locations [NONE|ALL|<LIST-OF-LOCATIONS>]
```

Parameters

- `allowed-locations <WORD> locations [NONE|ALL|<LIST-OF-LOCATIONS>]`

allowed-locations <WORD>	Configures a location tag and associates a list locations with the tag <WORD> – Provide a location tag not exceeding 32 characters in length.
locations [NONE|ALL|<LIST-OF-LOCATIONS>]	Associates locations with the above created location tag • NONE – When specified, states that none of the locations are to be allowed access. • ALL – When specified, states that all the locations are to be allowed access. • <LIST-OF-LOCATIONS> – Specifies a list of locations or individual RF Domains. When specified, states that the specified list of locations or RF Domain are allowed access.

Example

```
nx9500-6C8809(config-management-policy-test)#allowed-locations Ecospace locations
TechPubs ALL

nx9500-6C8809(config-management-policy-test)#allowed-locations TEST locations
NONE

nx9500-6C8809(config-management-policy-test)#show context
management-policy test
 no telnet
 no http server
 https server
 ssh
 allowed-location TEST locations NONE
 allowed-location Ecospace locations TechPubs ALL
nx9500-6C8809(config-management-policy-test)##
```

Related Commands

no	Removes the allowed-locations configuration

15.1.3 banner

management-policy

Configures the *message of the day* (motd) text. This text is displayed at login to clients connecting through Telnet or SSH.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
banner motd <LINE>
```

Parameters

- `banner motd <LINE>`

motd <LINE>	Sets the motd banner • <LINE> – Enter the message string. The message string should not exceed 255 characters.

Example

```
rfs6000-37FABE(config-management-policy-test)#banner motd "Have a Good Day"

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Removes the motd banner

15.1.4 ftp

management-policy

Enables *File Transfer Protocol* (FTP) on this management policy. FTP is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally. FTP access is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ftp {password|rootdir|username}

ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}

ftp {rootdir <DIR>}

ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir
<DIR>}
```

Parameters

- `ftp {password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>]}`

ftp password	Optional. Configures the FTP server password
1 <ENCRYPTED-PASSWORD>	Configures an encrypted password. Use this option when copy pasting the password from another device. • <ENCRYPTED-PASSWORD> – Specify the password. The password should not exceed 63 characters in length.
<PASSWORD>	Configures a clear text password

- `ftp {rootdir <DIR>}`

ftp rootdir <DIR>	Optional. Configures the root directory for FTP logins • <DIR> – Specify the root directory path. By default the root directory is set to flash:/

- `ftp {username <USERNAME> password [1 <ENCRYPTED-PASSWORD>|<PASSWORD>] rootdir <DIR>}`

ftp username <USERNAME>	Optional. Configures a new user account on the FTP server. The FTP user file lists users with FTP server access. • <USERNAME> – Specify the username. The username should not exceed 32 characters in length.

password 1 [<ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures an encrypted password • <ENCRYPTED-PASSWORD> – Specifies an encrypted password (use this option if copy pasting from another device). The password should not exceed 63 characters in length. • <PASSWORD> – Configures a clear text password
rootdir <DIR>	After specifying the password, configure the FTP root directory. • rootdir <DIR> – Configures the root directory for FTP logins. Specify the root directory path.

Usage Guidelines

The string size of an encrypted password (option 1, password is encrypted with a SHA1 algorithm) must be exactly 40 characters.

Example

```
rfs6000-37FABE(config-management-policy-test)#ftp username superuser password
test@123 rootdir dir

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Disables FTP and its settings, such as the server password, root directory, and users

15.1.5 http

management-policy

Enables *Hyper Text Transport Protocol* (HTTP) on this management policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
http server
```

Parameters

- `http server`

http server	Enables HTTP on this management policy. HTTP provides limited authentication and no encryption.

Example

```
rfs6000-37FABE(config-management-policy-test)#http server

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Disables HTTP on this management policy

15.1.6 https

management-policy

Enables *Hyper Text Transport Protocol Secure* (HTTPS) on this management policy

NOTE: If the a RADIUS server is not reachable, HTTPS management access to the controller or access point may be denied. RADIUS support is available locally on controllers and access points, with the exception of AP6511 and AP6522 models, which require an external RADIUS resource.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
https [server|sslv3|use-secure-ciphers-only]
```

Parameters

- `https [server|sslv3|use-secure-ciphers-only]`

https	Configures secure HTTP related parameters on this management policy
server	Enables HTTPS on this management policy. HTTPS provides both authentication and data encryption as opposed to just authentication. This option is enabled by default.
sslv3	Enables the use of SSLv3 protocol to connect to a Web page. When enabled, SSLv2 Web authentication is disabled, and enforces the use of Web browsers supporting SSLv3, which is a more secure protocol. This option is disabled by default.
use-secure-ciphers-only	Enables the use of TLS v1.2 ciphers to secure client-server network communications. When enabled, for HTTPS connections the TLS v1.2 protocol is used, instead of the less secure TLS v1.0 or TLS v1.1 protocols. This option is enabled by default.

Example

```
rfs6000-37FABE(config-management-policy-test)#https server

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 banner motd "Have a Good Day"
rfs6000-37FABE(config-management-policy-test)#
```

The following example shows that the ‘use-secure-ciphers-only’ option is enabled by default:

```
rfs6000-817379(config-management-policy-default)#show context include-factory |
incl https
https server
no https sslv3
https use-secure-ciphers-only
rfs6000-817379(config-management-policy-default)#
```

Related Commands

no	Disables HTTPS on this management policy

15.1.7 idle-session-timeout

management-policy

Configures a session's idle timeout. An idle session is automatically terminated after the specified interval is exceeded.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
idle-session-timeout <1-4320>
```

Parameters

- `idle-session-timeout <1-4320>`

<1-4320>	Sets the interval, in minutes, after which an idle session is timed out. Specify a value from 1 - 4320 minutes. The default is 30 minutes.

Example

```
rfs6000-37FABE(config-management-policy-test)#idle-session-timeout 100

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 100
 banner motd "Have a Good Day"
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Removes the configured idle session timeout value

15.1.8 ipv6

management-policy

Restricts management access to specified hosts and/or subnets based on their IPv6 addresses and prefixes respectively

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ipv6 restrict-access [host|ipv6-access-list|subnet]

ipv6 restrict-access host <IPv6> {log|subnet}
ipv6 restrict-access host <IPv6> {log [all|denied-only]}
ipv6 restrict-access host <IPv6> {subnet <IPv6-PREFIX> {log [all|denied-only]}}

ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>

ipv6 restrict-access subnet <IPv6-PREFIX> {host|log}
ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}
ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}
```

Parameters

- `ipv6 restrict-access host <IPv6> {log [all|denied-only]}`

host <IPv6>	Restricts management access to a specified host, based on the host's IPv6 address • <IPv6> – Specify the host's IPv6 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host is denied access)

- `ipv6 restrict-access host <IPv6> {subnet <IPv6-PREFIX> {log [all|denied-only]}}`

host <IPv6>	Restricts management access to a specified host, based on the host's IPv6 address. • <IPv6> – Specify the host's IPv6 address.
subnet <IPv6-PREFIX>	Optional. Restricts access to the host on a specified IPv6 subnet • <IPv6-PREFIX> – Specify the subnet's IPv6 prefix in the X:X::X:X/M format.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host/subnet is denied access)

- `ipv6 restrict-access ipv6-access-list <IPv6-ACCESS-LIST-NAME>`

ipv6-access-list <IPv6-ACCESS-LIST-NAME>	Uses an IPv6 *Access Control List* (ACL) to filter access requests. IPv6 ACLs filter/mark packets based on the IPv6 address from which they arrive. IPv6 hosts configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. An existing IPv6 ACL can be created and used in the management policy context to permit or deny access to specific hosts and/or subnets. • <IPv6-ACCESS-LIST-NAME> – Specify the IPv6 ACL name.

- `ipv6 restrict-access subnet <IPv6-PREFIX> {log [all|denied-only]}`

subnet <IPv6-PREFIX>	Restricts management access to a specified IPv6 subnet • <IPv6-PREFIX> – Specify the subnet's IPv6 prefix in the X:X::X:X/M format.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host/subnet is denied access)

- `ipv6 restrict-access subnet <IPv6-PREFIX> {host <IPv6> {log [all|denied-only]}}`

subnet <IPv6-PREFIX>	Restricts management access to a specified IPv6 subnet • <IPv6-PREFIX> – Specify the subnet's IPv6 prefix in the X:X::X:X/M format.
host <IPv6>	Optional. Restricts management access to a specific host within the specified subnet • <IPv6> – Specify the host's IPv6 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when a host/subnet is denied access)

Example

```
rfs6000-37FABE(config-management-policy-test)#ipv6 restrict-access host
2001:fdbc:06cf:0011::13 subnet 2001:fdbc:06cf:0011::0/64 log all

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 ipv6 restrict-access host 2001:fdbc:06cf:0011::13 subnet 2001:fdbc:06cf:0011::0/
64 log all
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Removes management access restriction settings

15.1.9 no

management-policy

Negates a command or reverts values to their default. When used in the config management policy mode, the `no` command negates or reverts management policy settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [aaa-login|allowed-locations|banner|ftp|http|https|idle-session-timeout|ipv6|
passwd-entry|privilege-mode-password|rest-server|restrict-access|snmp-server|
ssh|t5|telnet|user|service]

no aaa-login tacacs [accounting|authentication|authorization|fallback|policy]

no allowed-location <LOCATION-TAG>

no banner motd

no ftp {password|rootdir}

no http server

no https [server|sslv3|use-secure-ciphers-only]

no passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|
security-admin|superuser|system-admin|vendor-admin|web-user-admin]

no [idle-session-timeout|privilege-mode-password|rest-server|restrict-access]

no ipv6 restrict-access

no snmp-server [community|display-vlan-info-per-radio|enable|host|manager|
max-pending-requests|request-timeout|suppress-security-configuration-level|
throttle|user]

no snmp-server [community <WORD>|display-vlan-info-per-radio|enable traps|
host <IP> {<1-65535>}|manager [all|v1|v2|v3]|max-pending-requests|request-
timeout|suppress-security-configuration-level|throttle|user [snmpmanager|
snmpoperator|snmptrap]]

no ssh {login-grace-time|port|use-key}

no t5 snmp-server [community|enable|host]

no [telnet|user <USERNAME>]

no service prompt crash-info
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts this Management policy settings based on the parameters passed

Example

The following example shows the management policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 100
 banner motd "Have a Good Day"
rfs6000-37FABE(config-management-policy-test)#

rfs6000-37FABE(config-management-policy-test)#no banner motd
rfs6000-37FABE(config-management-policy-test)#no idle-session-timeout
rfs6000-37FABE(config-management-policy-test)#no http server
```

The following example shows the management policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
rfs6000-37FABE(config-management-policy-test)#
```

15.1.10 passwd-entry

management-policy

Configures user-account lockout and unlock parameters. Use this option to configure the maximum number of consecutive, failed login attempts allowed before an account is locked out, and the duration of lockout.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|
security-admin|superuser|system-admin|vendor-admin|web-user-admin] max-fail <1-
100> lockout-time <<0-600>
```

Parameters

```
• passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|
security-admin|superuser|system-admin|vendor-admin|web-user-admin] max-fail <1-
100> lockout-time <0-600>
```

passwd-entry role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|vendor-admin|web-user-admin] max-fail <1-100> lockout-time <<0-600>	Configures user-role based account lockout criteria • role – Select the user-role. The options are: • device-provisioning-admin • helpdesk • monitor • network-admin • security-admin • system-admin • vendor-admin • web-user-admin] • max-fail <1-100> – Specify the maximum number of consecutive, failed attempts allowed before an account is locked. Specify a value from 1 - 100. • lockout-time <<0-600> – Specify the maximum time, in minutes, for which an account remains locked. The value '0' indicates that the account is permanently locked. Specify a value from 0 - 600 minutes. When configured, the lockout is individually applied to each account within the specified role/roles. For example, consider the 'monitor' role having two users: 'user1' and 'user2'. The *max-fail* and *lockout-time* is set at '5' attempts and '10' minutes respectively. In this scenario, user2 makes 5 consecutive, failed login attempts, and the user2 account is locked out for 10 minutes. However, during this lockout time the user1 account remains active. **Note:** Note, in the event-system-policy context, enable 'login-lockout' and 'login-unlocked' event notification to trigger e-mail or syslog notification to users on occurrence of the *login-lockout* and *login-unlock* events. For more information, see *event*.

Example

```
rfs6000-817379(config-management-policy-default)#passwd-retry role monitor max-
fail 5 lockout-time 10

rfs6000-817379(config-management-policy-default)#show con
management-policy default
no telnet
no http server
https server
ssh
user admin password 1
979cfb9288837ee26d74d07b5ea328fd0e9a2b55cf5104649c2b496cc94e7003 role superuser
access all
passwd-retry role monitor max-fail 2 lockout-time 5
snmp-server community 0 private rw
snmp-server community 0 public ro
snmp-server user snmptrap v3 encrypted des auth md5 0 admin123
snmp-server user snmpmanager v3 encrypted des auth md5 0 admin123
rfs6000-817379(config-management-policy-default)#
```

Related Commands

no	Removes the user-account lockout and unlock parameters configured here

15.1.11 privilege-mode-password

management-policy

Configures the CLI's privilege mode access password. Use this option to strengthen security by enforcing a second level authentication to access the privilege configuration mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>
```

Parameters

- `privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>`

privilege-mode-password <PASSWORD/HASHED-STRING-ALIAS-NAME>	Configures the password required to enter the privilege configuration mode. When configured, users are prompted to provide the password when enabling the privilege configuration mode. • <PASSWORD/HASHED-STRING-ALIAS-NAME> – Enter the password as a clear text, or provide a hashed-string alias. Enter the password as a clear text, or provide a hashed-string alias. If using a hashed-string alias, ensure that the alias is existing and configured. Note, the clear text password is saved and displayed as a hashed string. Hashing is a means of establishing the integrity of transmitted messages. Before transmission, a hash of the message is generated, encrypted and sent along with the message. At the receiving end, the message and the hash are both decrypted, and another hash is generated from the received message. The two hashes are compared. If both are identical the message is considered to have been transmitted intact. **Note:** For more information on configuring a hashed-string alias, see *alias*.

Example

The following example shows the privilege mode password being configured as a hashed string:

```
rfs6000-37FABE(config-management-policy-test)#privilege-mode-password 1
2e9f038ac2ed27f919ed5a4dceb3d30e32f356f2ceff6fbf26a153d0339c734f

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 privilege-mode-password 1
2e9f038ac2ed27f919ed5a4dceb3d30e32f356f2ceff6fbf26a153d0339c734f
rfs6000-37FABE(config-management-policy-test)#
```

Follow the steps below to configure a hashed-string alias and use it as a privilege mode password:

1 In the global-configuration context, create a hashed-string alias.

```
nx9500-6C8809(config)#alias hashed-string $PriMode Test12345

nx9500-6C8809(config)#show context | include alias
alias vlan $BLR-01 1
alias string $IN-Blr-EcoSpace-Floor-4 IBEF4
alias encrypted-string $READ 0 public
alias encrypted-string $WRITE 0 private
alias hashed-string $PriMode 1
faffdde27cb49ad634ea20df4f7c8ef2685894d10ffcb1b2efba054112ecfc75
nx9500-6C8809(config)#
```

2 In the management-policy context, configure the hashed-string alias created in step 1 as the privilege mode password.

```
nx9500-6C8809(config-management-policy-test)#privilege-mode-password $PrivMode

nx9500-6C8809(config-management-policy-default)#show context
management-policy default
https server
 rest-server
 ssh
 user admin password 1
ad4d8797f007444ccdda3788b9ee0e8b46f3facb4308e045239eb7771e127ed5 role
superuser access all
 snmp-server community 0 $WRITE rw
 snmp-server community 0 $READ ro
 snmp-server user snmptrap v3 encrypted des auth md5 2 yqr96yyVzmD4ZbU2I7Eh/
QAAAAjWNKa4KXF95pruUCSnhOiT
 snmp-server user snmpmanager v3 encrypted des auth md5 2 NOf8+2+AY2r4ZbU2I7Eh/
QAAAAgc0l8ahJYo3AjHo9wXzYGo
 t5 snmp-server community public ro 192.168.0.1
 t5 snmp-server community private rw 192.168.0.1
 privilege-mode-password $PriMode
nx9500-6C8809(config-management-policy-default)#
```

3 Confirm, if the privilege mode is password protected.

```
nx9500-6C8809 login: admin
Password:
Feb 07 14:40:47 2017: %AUTH-6-INFO: login[28768]: user 'admin' on 'ttyS0' from
'Console' logged in
Feb 07 14:40:47 2017: nx9500-6C8809 : %SYSTEM-5-LOGIN: Successfully logged in
user 'admin' with privilege 'superuser' from 'ttyS0'
nx9500-6C8809>en
Password:
```

Related Commands

no	Removes the configured CLI privilege mode access password

15.1.12 rest-server

management-policy

Enables the *Representational State Transfer* (REST) server. When enabled, the REST server allows vendor users access to the online device registration portal. All requests and responses to and from the on-boarding portal are handled by the REST server through restful *Application Programming Interface* (API) transactions. The REST server serves the Web pages used to associate a device's MAC address with a specific vendor group.

Each vendor has a 'vendor-admin' user who is assigned a unique, username/password credential for RADIUS server validation. Successfully validated vendor-admins can access the online device registration portal to on-board devices. For more information on vendor-admin user configuration, see *user*.

The REST server is enabled by default.

Supported in the following platforms:

- Service Platforms — NX9500, NX9510, NX9600, VX9000

Syntax

```
rest-server
```

Parameters

None

Example

```
nx9500-6C8809(config-management-policy-testMNGTPolicy)#show context
management-policy testMNGTPolicy
 no telnet
 no http server
 https server
 rest-server
 ssh
nx9500-6C8809(config-management-policy-testMNGTPolicy)#

nx9500-6C8809(config-management-policy-testMNTPolicy)#no rest-server

nx9500-6C8809(config-management-policy-testMNGTPolicy)#show context
management-policy testMNGTPolicy
 no telnet
 no http server
 https server
 no rest-server
 ssh
nx9500-6C8809(config-management-policy-testMNGTPolicy)#
```

Related Commands

no	Disables the REST server

15.1.13 restrict-access

management-policy

Restricts management access to a set of hosts or subnets

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access). Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
restrict-access [host|ip-access-list|subnet]

restrict-access host <IP> {log|subnet}
restrict-access host <IP> {log [all|denied-only]}
restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}

restrict-access ip-access-list <IP-ACCESS-LIST-NAME>

restrict-access subnet <IP/M> {host|log}
restrict-access subnet <IP/M> {log [all|denied-only]}
restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}
```

Parameters

- `restrict-access host <IP> {log [all|denied-only]}`

host <IP>	Restricts management access to a specified host, based on the host's IPv4 address • <IP> – Specify the host's IPv4 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access (when an access request is received from a host denied access, a record is logged)

- `restrict-access host <IP> {subnet <IP/M> {log [all|denied-only]}}`

host <IP>	Restricts management access to a specified host, based on the host's IPv4 address • <IP> – Specify the host's IPv4 address.
subnet <IP/M>	Optional. Restricts access to the host on a specified subnet • <IP/M> – Specify the subnet's IPv4 address and mask in the A.B.C.D/M format.

log [all|denied-only]	Optional. Configures a logging policy for access requests. • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when access request received from a host is denied)

- `restrict-access ip-access-list <IP-ACCESS-LIST-NAME>`

ip-access-list	Uses an IPv4 ACL to filter access requests IPv4 ACLs filter/mark packets based on the IPv4 address from which they arrive. IP and non-IP traffic, on the same layer 2 interface, can be filtered by applying an IPv4 ACL. Each IPv4 ACL contains a set of deny and/or permit rules. Each rule is specific to source and destination IPv4 addresses and the unique rules and precedence definitions assigned. When the network traffic matches the criteria specified in one of these rules, the action defined in that rule is used to determine whether the traffic is allowed or denied.
<IP-ACCESS-LIST-NAME>	Specify the IPv4 ACL name.

- `restrict-access subnet <IP/M> {log [all|denied-only]}`

subnet <IP/M>	Restricts management access to a specified subnet • <IP/M> – Specify the subnet's IPv4 address and mask in the A.B.C.D/M format.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when access request received from a subnet is denied)

- `restrict-access subnet <IP/M> {host <IP> {log [all|denied-only]}}`

subnet <IP/M>	Restricts management access to a specified subnet • <IP/M> – Specify the subnet's IPv4 address and mask in the A.B.C.D/M format
host <IP>	Optional. Uses the host IP address as a second filter • <IP> – Specify the host's IPv4 address.
log [all|denied-only]	Optional. Configures a logging policy for access requests. Sets the log type generated for access requests • all – Logs all access requests, both denied and permitted • denied-only – Logs only denied access events (when access request received from a host within the specified subnet is denied)

Example

```
rfs6000-37FABE(config-management-policy-test)#restrict-access host 172.16.10.4
log denied-only

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.4 log denied-only
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Removes device access restrictions

15.1.14 snmp-server

management-policy

Configures the *Simple Network Management Protocol* (SNMP) engine settings. SNMP is an application layer protocol that facilitates the exchange of management information between the controller and a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the controller's management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string gathers statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system's performance and other parameters.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
snmp-server [community|enable|display-vlan-info-per-radio|host|manager|max-
pending-requests|request-timeout|suppress-security-configuration-level|
throttle|user]

snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw] {ip-snmp-access-list <IP-
SNMP-ACL-NAME>}

snmp-server enable traps

snmp-server host <IP> [v1|v2c|v3] {<1-65535>}

snmp-server manager [all|v1|v2|v3]

snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]

snmp-server [display-vlan-info-per-radio|throttle <1-100>|suppress-security-
configuration-level [0|1]]

snmp-server user [snmpmanager|snmpoperator|snmptrap]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth|encrypted]

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD>|2
<ENCRYPTED-PASSWORD>|<PASSWORD>]

snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted [auth md5|des
auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]
```

Parameters

- `snmp-server community [0 <WORD>|2 <WORD>|<WORD>] [ro|rw] {ip-snmp-access-list <IP-SNMP-ACL-NAME>}`

community [0 <WORD>| 2 <WORD>| <WORD>]	Sets the community string and associated access privileges. Define a public or private community designation. By default, SNMPv2 community strings on most devices are set to *public* for the *read-only* community string, and *private* for the *read-write* community string. • 0 <WORD> – Sets a clear text SNMP community string • 2 <WORD> – Sets an encrypted SNMP community string • <WORD> – Sets the SNMP community string
[ro|rw]	After configuring the SNMP community string, set the access permission for each community string used by devices to retrieve or modify information. Available options include • ro – Assigns read-only access to the specified SNMP community (allows a remote device to retrieve information) • rw – Assigns read and write access to the specified SNMP community (allows a remote device to modify settings)
ip-snmp-access-list <IP-SNMP-ACL-NAME>	Optional. Associates an IP SNMP access list (should be existing and configured). The IP SNMP ACL sets the SNMP management station's IP address. SNMP trap information is received at this address.

- `snmp-server enable traps`

enable traps	Enables trap generation (using the trap receiver configuration defined). This feature is disabled by default. Enabling this feature ensures the dispatch of SNMP notifications to all hosts. In a managed network, the controller uses SNMP trap receivers to notify faults. SNMP traps are unsolicited notifications triggered by thresholds (or actions) on devices and are therefore an important fault management tool. A SNMP trap receiver is the destination of SNMP messages (external to the controller). A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community, etc. SNMP trap notifications exist for most controller operations, but not all are necessary for day-to-day operation.

- `snmp-server host <IP> [v1|v2c|v3] {<1-65535>}`

host <IP>	Configures a host's IP address. This is the external server resource dedicated to receiving SNMP traps on behalf of the controller.
[v1|v2c|v3]	Configures the SNMP version used to send the traps • v1 – Uses SNMP version 1. This option is disabled by default. • v2c – Uses SNMP version 2c. This option is disabled by default. • v3 – Uses SNMP version 3. This option is enabled by default.

<1-65535>	Optional. Configures the virtual port of the server resource dedicated to receiving SNMP traps • <1-65535> – Optional. Specify a value from 1 - 65535. The default port is 162.

- `snmp-server manager [all|v1|v2|v3]`

manager [all|v2|v3]	Enables SNMP manager and specifies the SNMP version • all – Enables SNMP manager version v2 and v3 • v1 – Enables SNMP manager version v1 only. SNMPv1 uses a simple password ("community string"). Data is unencrypted (clear text). Consequently it provides limited security, and should be used only inside LANs behind firewalls, not in WANs. • v2 – Enables SNMP manager version v2 only. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses *Get*, *GetNext*, and *Set* operations for data management. SNMPv2 is enabled by default. • v3 – Enables SNMP manager version v3 only. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *User-based Security Model* (USM) for message security and the *View-based Access Control Model* (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

- `snmp-server [max-pending-requests {<64-1024>}|request-timeout {<2-720>}]`

max-pending-requests {<64-1024>}	Sets the maximum number of requests that can be pending at any given time • <64-1024> – Optional. Specify a value from 64 - 1024. The default is 128.
request-timeout {<2-720>}	Sets the interval, in seconds, after which an error message is returned for a pending request • <2-720> – Optional. Specify a value from 2 - 720 seconds. The default is 240 seconds.

- `snmp-server [display-vlan-info-per-radio|throttle <1-100>|suppress-security-configuration-level [0|1]]`

display-vlan-info-per-radio	Enables the display of the VLAN ID along with the radio interface ID
throttle <1-100>	Sets CPU usage for SNMP activities. Use this command to set the CPU usage from 1 - 100.

suppress-security-configuration-level [0|1]	Sets the level of suppression of SNMP security configuration information
	• 0 – If this option is selected, an empty string is returned for the SNMP request for security configuration information. Security configuration information consists of:
	  • Passwords
	  • Keys
	  • Shared secrets
	The default setting is 0.
	• 1 – Suppresses the display of the policy, IP ACL, passwords, keys and shared secrets. If this option is selected, in addition to suppression from 'Level 0', an empty string is returned for a SNMP request on following items:
	  • Management policies
	  • IP ACL
	  • Tables containing user names and community strings

• `snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 auth md5 [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]`

user [snmpmanager| snmpoperator| snmptrap]	Defines user access to the SNMP engine • snmpmanager – Sets user as a SNMP manager • snmpoperator – Sets user as a SNMP operator • snmptrap – Sets user as a SNMP trap user
v3 auth md5	Uses SNMP version 3 as the security model • auth – Uses an authentication protocol • md5 – Uses HMAC-MD5 algorithm for authentication
[0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures password using one of the following options: • 0 <PASSWORD> – Configures clear text password • 2 <ENCRYPTED - PASSWORD> – Configures encrypted password • <PASSWORD> – Specifies a password for authentication and privacy protocols

• `snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 encrypted [auth md5|des auth md5] [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>]`

user [snmpmanager| snmpoperator| snmptrap]	Defines user access to the SNMP engine • snmpmanager – Sets user as a SNMP manager • snmpoperator – Sets user as a SNMP operator • snmptrap – Sets user as a SNMP trap user
v3 encrypted	Uses SNMP version 3 as the security model • encrypted – Uses encrypted privacy protocol
auth md5	Uses authentication protocol • auth – Sets authentication parameters • md5 – Uses HMAC-MD5 algorithm for authentication

des auth md5	Uses privacy protocol for user privacy
	• des – Uses CBC-DES for privacy
	After specifying the privacy protocol, specify the authentication mode.
	  • auth – Sets user authentication parameters
	  • md5 – Uses HMAC-MD5 algorithm for authentication

[0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	The following are common to both the auth and des parameters: Configures password using one of the following options: • 0 <PASSWORD> – Configures a clear text password • 2 <ENCRYPTED - PASSWORD> – Configures an encrypted password • <PASSWORD> – Specifies a password for authentication and privacy protocols

Example

```
rfs6000-37FABE(config-management-policy-test)#snmp-server community snmp1 ro

rfs6000-37FABE(config-management-policy-test)#snmp-server host 172.16.10.23 v3
162

rfs6000-37FABE(config-management-policy-test)#commit

rfs6000-37FABE(config-management-policy-test)#snmp-server user snmpmanager v3
auth md5 test@123

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 no ssh
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Disables or resets the SNMP server settings

15.1.15 ssh

management-policy

Enables *Secure Shell* (SSH) for this management policy

SSH, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.

NOTE: If the a RADIUS server is not reachable, SSH management access to the controller or access point may be denied. RADIUS support is available locally on controllers and access points, with the exception of AP6511 and AP6522 models, which require an external RADIUS resource.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ssh {login-grace-time <60-300>|port <1-65535>}
```

Parameters

- `ssh {login-grace-time <60-300>|port <1-65535>}`

ssh	Enables SSH communication between client and server
login-grace-time <60-300>	Optional. Configures the login grace time. This is the interval, in seconds, after which an unsuccessful login is disconnected. • <60-300> – Specify a value from 60 - 300 seconds. The default is 60 seconds.
port <1-65535>	Optional. Configures the SSH port. This is the port used for SSH connections. • <1-65535> – Specify a value from 1 - 165535. The default port is 22.

Example

```
rfs6000-37FABE(config-management-policy-test)#ssh port 162

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 no http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 ssh port 162
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Resets SSH access port to factory default (port 22)

15.1.16 t5

management-policy

Configures SNMP server settings for T5 devices on this management policy

A T5 controller is an external device that can be adopted and managed by a WiNG controller. When enabled as a supported external device, a T5 controller can provide data to WiNG to assist in it's management within a WiNG supported subnet.

This command enables SNMP to communicate with T5 devices within the network. SNMP facilitates the exchange of management information between the controller or service platform and the T5 device. For more information, see *snmp-server*.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510

Syntax

```
t5 snmp-server [community|contact|enable|host|location]
t5 snmp-server community <COMMUNITY-NAME> [ro|rw] <SNMP-STATION-IP>
t5 snmp-server contact <LINE>
t5 snmp-server enable [server|traps]
t5 snmp-server host <IP>
t5 snmp-server location <LINE>
```

Parameters

- `t5 snmp-server community <COMMUNITY-NAME> [ro|rw] <SNMP-STATION-IP>`

community <COMMUNITY-NAME> [ro|rw]	Defines a public or private community designation. By default, SNMPv2 community strings on most devices are set to public, for the read-only community string, and private for the read-write community string.
	• <COMMUNITY-NAME> – Specify the SNMP community name, and configure the access permission for this community string (used by devices to retrieve or modify information).
	  • ro – Allows a remote device to retrieve information only
	  • rw – Allows a remote device to retrieve information and modify settings

<SNMP-STATION-IP>	Specify the SNMP management station IP address for receiving trap information

- `t5 snmp-server contact <LINE>`

contact <LINE>	Configures the administrator of SNMP trap events for the T5 controller. • <LINE> – Specify the administrator's name (should not exceed 64 characters).

- `t5 snmp-server enable [server|traps]`

enable [server|traps]	Enables the following: • server – Enables the SNMP server. When enabled, the system accepts SNMP management data. This is enabled by default. • traps – Enables SNMP traps. When enabled, the system generates SNMP traps. This is enabled by default.

- `t5 snmp-server host <IP>`

host <IP>	Configures the T5 SNMP host's IP address. The SNMP host receives the SNMP notifications. • <IP> – Specify the SNMP host's IP address.

- `t5 snmp-server location <LINE>`

location <LINE>	Configures the system location for SNMP traps. • <LINE> – Specify the SNMP trap location (should not exceed 64 characters).

Example

```
nx9500-6C8809(config-management-policy-test)#t5 snmp-server community lab rw
192.168.13.7

nx9500-6C8809(config-management-policy-test)#show context
management-policy test
 http server
 no ssh
 t5 snmp-server community lab rw 192.168.13.7
nx9500-6C8809(config-management-policy-test)#
```

Related Commands

no	Removes or reverts SNMP server configuration for T5 devices

15.1.17 telnet

management-policy

Enables Telnet. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.

By default Telnet, when enabled, uses *Transmission Control Protocol* (TCP) port 23. Use this command to change the TCP port.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
telnet {port <1-65535>}
```

Parameters

- `telnet {port <1-65535>}`

telnet	Enables Telnet
port <1-65535>	Optional. Configures the Telnet port. This is the port used for Telnet connections. • <1-65535> – Sets a value from 1 - 65535. The default port is 23.

Example

```
rfs6000-37FABE(config-management-policy-test)#telnet port 200

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 telnet port 200
 no http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 ssh port 162
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
 snmp-server host 172.16.10.23 v3 162
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs6000-37FABE(config-management-policy-test)#
```

Related Commands

no	Disables Telnet

15.1.18 user

management-policy

Adds new user account. Use this option to add a new user, and define the role, access type, and allowed locations assigned to the user.

Management services like Telnet, SSHv2, HTTP, HTTPs and FTP require users (administrators) enter a valid username and password, which is authenticated locally or centrally on a RADIUS server. SNMPv3 also requires a valid username and password, which is authenticated by the SNMPv3 module. For CLI users, the controller or service platform also requires user role information to know what permissions to assign.

- If local authentication is used, associated role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor-specific return attributes. If no role information is supplied by RADIUS, the controller or service platform applies default read-only permissions.

Administrators can limit users to specific management interfaces. During authentication, the controller or service platform looks at the user's access assignment to determine if the user has permissions to access an interface:

- If local authentication is used, role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor-specific return attributes.

The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller or service platform can also deny the authentication request if the user is attempting to access a management interface not specified in the account's access mode list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role [device-
provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|vendor-admin|web-user-admin]

user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role [device-
provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|web-user-admin] access [all|console|ssh|telnet|web]
({allowed-locations <ALLOWED-LOCATIONS>})

user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role vendor-
admin group <VENDOR-GROUP-NAME>
```

Parameters

```
• user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role
[device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|
superuser|system-admin|web-user-admin] access [all|console|ssh|telnet|web]
({allowed-locations <ALLOWED-LOCATIONS>})
```

user <USERNAME>	Adds a new user account to this management policy • <USERNAME> – Sets the username. This is a mandatory field and cannot exceed 32 characters. Assign a name representative of the user and the intended role.
password [0 <PASSWORD>| 1 <SHA1-PASSWORD>| <PASSWORD>]	Configures a password • 0 <PASSWORD> – Sets a clear text password • 1 <SHA1-PASSWORD> – Sets the SHA1 hash of the password • <PASSWORD> – Sets the password
role	Configures the user role. The options are: • device-provisioning-admin – Device provisioning administrator. Has privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a devices existing configuration unless the configuration is properly archived. • helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as run troubleshooting utilities (like a sniffer), view/retrieve logs, clear statistics, reboot, create and copy technical support dumps. The helpdesk administrator can also create a guest user account and password for registration. However, the helpdesk admin cannot execute controller or service platform reloads. • monitor – Monitor. Has read-only access to the system. Can view configuration and statistics except for secret information. • network-admin – Network administrator. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF • security-admin – Security administrator. Modifies WLAN keys and passphrases • superuser – Superuser. Has full access, including halt and delete startup-config • system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access • web-user-admin – Web user administrator. This role is used to create guest users and credentials. The Web user admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.
access [all|console|ssh| telnet|web]	Configures the access type • all – Allows all types of access: console, SSH, Telnet, and Web • console – Allows console access only • ssh – Allows SSH access only • telnet – Allows Telnet access only • web – Allows Web access only
allowed-locations <ALLOWED-LOCATIONS>	Optional. This keyword is recursive and optional. It configures a list of locations (either as a path or a RF Domain) to which this user is allowed access. • <ALLOWED-LOCATIONS> – Specify the allowed locations. **Note:** Use this option to configure a list of RF Domains or its tree nodes to which this user is allowed access with respect to the Nsight policy. **Note:** This option is not applicable to the user role 'web-user-admin'.

```
• user <USERNAME> password [0 <PASSWORD>|1 <SHA1-PASSWORD>|<PASSWORD>] role
vendor-admin group <VENDOR-GROUP-NAME>
```

user <USERNAME>	Adds a new user account to this management policy • <USERNAME> – Sets the username. This is a mandatory field and cannot exceed 32 characters. Assign a name representative of the user and the intended role.
password [0 <PASSWORD>| 1 <SHA1-PASSWORD>| <PASSWORD>]	Configures a password • 0 <PASSWORD> – Sets a clear text password • 1 <SHA1-PASSWORD> – Sets the SHA1 hash of the password • <PASSWORD> – Sets the password
role vendor-admin	Configures this user's role as vendor-admin. Once created, the vendor-admin can access the online device-registration portal to add devices to the RADIUS vendor group to which he/she belongs. Vendor-admins have *only* Web access to the device registration portal. The WiNG software allows multiple vendors to securely on-board their devices through a single SSID. Each vendor has a 'vendor-admin' user who is assigned a unique, username/password credential for RADIUS server validation. Successfully validated vendor-admins can on-board their devices, which are, on completion of the on-boarding process, immediately placed on the vendor-allowed VLAN. On subsequent associations with this SSID, registered devices are dynamically placed into the vendor-allowed VLAN. If assigning the vendor-admin role, provide the vendor's group name for RADIUS authentication. The vendor's group takes precedence over the statically configured group for device registration. **Note:** Use the *service > show > wireless > credential-cache* command to view on-boarded device's VLAN assignment. **Note:** Ensure that the REST server is enabled, to allow vendor users access to the online device registration portal. Note, by default the REST server is enabled. For more information, see *rest-server*.
group <VENDOR-GROUP-NAME>	Associates this vendor-admin user with a vendor group, required for RADIUS authentication. The vendor group should be existing and configured in the RADIUS group policy. For more information on configuring RADIUS groups, see *radius-group*. • <VENDOR-GROUP-NAME> – Provide the vendor group name. In case of multiple allowed groups, provide a list of comma-separated group names.

Example

```
rfs6000-37FABE(config-management-policy-test)#user TESTER password test123 role
superuser access all

rfs6000-37FABE(config-management-policy-test)#show context
management-policy test
 telnet port 200
 no http server
 https server
 ftp username superuser password 1
f617ca50c59fb47028f96db4baab5f3d8f03c03ab257960b0fd127c69f02cd7e rootdir dir
 ssh port 162
 user TESTER password 1
b6b37c51405f4e93c67fe8af82d450c9fd6af69324cd56a55055cefe695b6a14 role superuser
access all
 snmp-server community snmp1 ro
 snmp-server user snmpmanager v3 encrypted des auth md5 0 test@123
 snmp-server host 172.16.10.23 v3 162
```

```
 aaa-login radius external
 aaa-login radius policy test
 idle-session-timeout 0
 restrict-access host 172.16.10.2 log all
rfs6000-37FABE(config-management-policy-test)#

nx9500-6C8809(config-management-policy-OB)#user test password 0 test123 role
vendor-admin group Apple,Sony,Samsung

nx9500-6C8809(config-management-policy-OB)#user Samsung password 0 samsung
role vendor-admin group Samsung

nx9500-6C8809(config-management-policy-OB)#show context
management-policy OB
 no telnet
 no http server
 https server
 rest-server
 ssh
 user admin password 1
d9849649218dcaa79109fbd47bbf1a24ecdf1edda220d21f76ce4c15a4e7e696 role superuser
access all
 user test password 1
62fca173a1ffc0e9cc4eef782b1978a5e0c47f66bc57a32992f03e3e00fe0bc4 role vendor-
admin group Apple,Sony,Samsung
 user Samsung password 1
39cb036b8e09c2ec625ebcda6e4001f4584263ed86fa69fc1f6b284113772eb0 role vendor-
admin group Samsung
nx9500-6C8809(config-management-policy-OB)#
```

Related Commands

no	Removes a user account

15.1.19 service

management-policy

Invokes service commands

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
service [prompt|show]
service [prompt crash-info|show cli]
```

Parameters

- `service [prompt crash-info|show cli]`

service prompt crash-info	Updates CLI prompt settings • crash-info – Includes an asterix at the end of the prompt if the device has crash files in the flash:/crashinfo folder
service show cli	Displays running system information • cli – Displays the current mode's CLI tree

Example

```
rfs6000-37FABE(config-management-policy-test)#service show cli
Management Mode mode:
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
  +-commands [show commands]
  +-simulate
    +-stats [show simulate stats]
  +-eval
    +-WORD [show eval WORD]
  +-debugging [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-cfgd [show debugging cfgd]
    +-on
      +-DEVICE-OR-DOMAIN-NAME [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]
    +-fib [show debugging fib(|(on DEVICE-NAME))]
      +-on
        +-DEVICE-NAME [show debugging fib(|(on DEVICE-NAME))]
    +-wireless [show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))]
      +-on
--More--
```

Related Commands

no	Disables the inclusion of an asterix indicator notifying the presence of crash files

16 RADIUS-POLICY

This chapter summarizes the RADIUS group, server, and user policy commands in the CLI command structure.

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to authenticate users and authorize their access to the network. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the local RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to a network, the authentication request is sent to the local RADIUS server. The authentication and encryption of communications takes place through the use of a shared secret password (not transmitted over the network).

The local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assigns policies for group authorization.

Controllers and access points allow enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. A certificate is required for EAP TTLS, PEAP, and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after RADIUS server authentication. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

The chapter is organized into the following sections:

- *radius-group*
- *radius-server-policy*
- *radius-user-pool-policy*

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

16.1 radius-group

RADIUS-POLICY

This section describes RADIUS user group configuration commands.

The local RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the local database. The user ID in the received access request is mapped to the associated wireless group for authentication. The configuration of groups allows enforcement of the following policies that control user access:

- Assign a VLAN to the user upon successful authentication
- Define start and end of time (HH:MM) when the user is allowed to authenticate
- Define the SSID list to which a user, belonging to this group, is allowed to associate
- Define the days of the week the user is allowed to login
- Rate limit traffic (for non-management users)

RADIUS users are categorized into three groups: normal user, management user, and guest user. A RADIUS group not configured as management or guest is a normal user group. User access and role settings depends on the RADIUS group the user belongs.

Use the (config) instance to configure RADIUS group commands. This command creates a group within the existing RADIUS group. To navigate to the RADIUS group instance, use the following commands:

```
<DEVICE>(config)#radius-group <GROUP-NAME>

rfs6000-37FABE(config)#radius-group test
rfs6000-37FABE(config-radius-group-test)#?
Radius user group configuration commands:
  guest       Make this group a Guest group
  no          Negate a command or set its defaults
  policy      Radius group access policy configuration
  rate-limit  Set rate limit for group

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs6000-37FABE(config-radius-group-test)#
```

NOTE: The RADIUS group name cannot exceed 32 characters, and cannot be modified as part of the group edit process.

The following table summarizes RADIUS group configuration commands:

Table 16.1 *RADIUS-Group-Config Commands*

Command	Description	Reference
guest	Enables guest access for the newly created group	*page 16-4*
no	Negates a command or reverts settings to their default	*page 16-10*
policy	Configures RADIUS group access policy parameters	*page 16-5*
rate-limit	Sets the default rate limit per user in Kbps, and applies it to all enabled WLANs	*page 16-9*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

16.1.1 guest

radius-group

Configures this group as a guest (non-management) group. A guest user group has temporary permissions to the controller's local RADIUS server. You can configure multiple guest user groups, each having a unique set of settings. Guest user groups cannot be made management groups with access and role permissions.

Guest users and policies are used for captive portal authorization to the network.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
guest
```

Parameters

None

Example

```
rfs6000-37FABE(config-radius-group-test)#guest

rfs6000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
rfs6000-37FABE(config-radius-group-test)#
```

Related Commands

no	Makes this group a non-guest group

16.1.2 policy

radius-group

Sets a RADIUS group's authorization settings, such as access day/time, WLANs, etc.

NOTE: A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
policy [access|day|inactivity-timeout|role|session-time|ssid|time|vlan]

policy vlan <1-4094>

policy access [all|console|ssh|telnet|web]

policy access [all|console|ssh|telnet|web] {(all|console|ssh|telnet|web)}

policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|
weekdays)}

policy inactivity-timeout <60-86400>

policy role [device-provisioning-admin|helpdesk|monitor|network-admin|security-
admin|superuser|system-admin|web-user-admin]

policy session-time <5-144000>

policy ssid <SSID>

policy time start <HH:MM> end <HH:MM>
```

NOTE: Access and role settings are applicable only to a management group. They cannot be configured for a RADIUS non-management group.

Parameters

- `policy vlan <1-4094>`

vlan <1-4094>	Sets the guest RADIUS group's VLAN ID from 1 - 4094. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server). This option applicable to a guest user group, which has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each group. Guest user groups cannot be made management groups with unique access and role permissions. Enable dynamic VLAN assignment for the WLAN for the VLAN assignment to take effect.

- `policy access [all|console|ssh|telnet|web] {(all|console|ssh|telnet|web)}`

access	Configures access type for a management group. Management groups can be assigned unique access and role permissions. • all – Allows all access. Wireless client access to the console, ssh, telnet, and/or Web • console – Allows console access only • ssh – Allows SSH access only • telnet – Allows Telnet access only • web – Allows Web access only These parameters are recursive, and you can provide access to more than one component.

- `policy role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]`

role [device-provisioning-admin|helpdesk|monitor|network-admin|security-admin|superuser|system-admin|web-user-admin]	Configures the role assigned to a management RADIUS group. If a group is listed as a management group, it may also have a unique role assigned. Available roles include: • device-provisioning-admin – Device provisioning administrator. Has privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a devices existing configuration unless the configuration is properly archived. • helpdesk – Helpdesk administrator. Performs troubleshooting tasks, such as clear statistics, reboot, create and copy tech support dumps. The helpdesk administrator can also create a guest user account and password for registration. These details can be e-mailed or sent as SMS to a mobile phone. • monitor – Monitor. Has read-only access to the network. Can view configuration and statistics except for secret information • network-admin – Network administrator. has wired and wireless access to the network. Manages layer 2, layer 3, Wireless, RADIUS server, DHCP server, and Smart RF • security-admin – Security administrator. Has full read/write access to the network. Modifies WLAN keys and passphrases • superuser – Superuser. Has full access, including halt and delete startup config • system-admin – System administrator. Upgrades image, boot partition, time, and manages admin access • web-user-admin – Web user administrator. This role is used to create guest users and credentials. The web-user-admin can access only the custom GUI screen and does not have access to the normal CLI and GUI.

- `policy inactivity-timeout <60-86400>`

inactivity-timeout <60-86400>	Configures the inactivity time for this RADIUS group users. If a frame is not received from a client for the specified period, then the client's session is removed. When defined, this value is used instead of the captive-portal inactivity timeout. If the inactivity timeout is not configured in the radius-group context or the captive-portal context, the default timeout (60 seconds) is applied. • <60-86400> – Specify a value from 60 - 86400 seconds. This option is disabled by default.

- `policy session-time <5-144000>`

session-time <5-144000>	Configures the session duration for client's belonging to a specific vendor group. Once configured, this is the duration for which over-the-air, on-boarded, successfully authenticated devices, belonging to a vendor group, get online access. The session is removed on completion of this duration. The vendor's RADIUS group takes precedence over statically configured group for device registration. • <5-144000> – Specify a value from 5 - 144000 minutes. This option is disabled by default. For more information, see *configuring device registration with dynamic VLAN assignment*.

- `policy ssid <SSID>`

ssid <SSID>	Sets the *Service Set Identifier* (SSID) for this guest RADIUS group. Use this command to assign SSIDs that users within this RADIUS group are allowed to associate. Assign SSIDs of those WLANs only that the guest users need to access. This option is not available for a management group. • <SSID> – Specify a case-sensitive alphanumeric SSID, not exceeding 32 characters.

- `policy day [all|fr|mo|sa|su|th|tu|we|weekdays] {(fr|mo|sa|su|th|tu|we|weekdays)}`

day [all|fr|mo|sa|su|th|tu|we|weekdays]	Configures the days on which this guest RADIUS group members can access the local RADIUS resources. The options are recursive, and you can provide access on multiple days. • fr – Allows access on Friday only • mo – Allows access on Mondays only • sa – Allows access on Saturdays only • su – Allows access on Sundays only • th – Allows access on Thursdays only • tu – Allows access on Tuesdays only • we – Allows access on Wednesdays only • weekdays – Allows access on weekdays only (Monday to Friday)

- `policy time start <HH:MM> end <HH:MM>`

time start<HH:MM> end <HH:MM>	Configures the time when this RADIUS group can access the network • start <HH:MM> – Sets the start time in the HH:MM format (for example, 13:30 means the user can login only after 1:30 PM). Specifies the time users, within each listed group, can access the local RADIUS resources. • end <HH:MM> – Sets the end time in the HH:MM format (for example, 17:30 means the user is allowed to remain logged in until 5:30 PM). Specifies the time users, within each listed group, lose access to the local RADIUS resources.

Usage Guidelines

A management group access policy provides:

- access details
- user roles
- policy's start and end time

The SSID, day, and VLAN settings are not applicable to a management user group.

Example

The following example shows a RADIUS guest group settings:

```
rfs6000-37FABE(config-radius-group-test)#policy time start 13:30 end 17:30
rfs6000-37FABE(config-radius-group-test)#policy day all
rfs6000-37FABE(config-radius-group-test)#policy vlan 1
rfs6000-37FABE(config-radius-group-test)#policy ssid test

rfs6000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid test
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 policy time start 13:30 end 17:30
rfs6000-37FABE(config-radius-group-test)#
```

The following example shows a RADIUS management group settings:

```
rfs6000-37FABE(config-radius-group-management)#policy access console ssh telnet
rfs6000-37FABE(config-radius-group-management)#policy role network-admin
rfs6000-37FABE(config-radius-group-management)#policy time start 9:30 end 20:30

rfs6000-37FABE(config-radius-group-management)#show context
radius-group management
 policy time start 9:30 end 20:30
 policy access console ssh telnet web
 policy role network-admin
rfs6000-37FABE(config-radius-group-management)#
```

Related Commands

no	Removes or modifies a RADIUS group's access settings

16.1.3 rate-limit

radius-group

Sets the rate limit for the guest RADIUS server group

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
rate-limit [from-air|to-air] <100-1000000>
```

NOTE: The rate-limit setting is not applicable to a management group.

Parameters

- `rate-limit [from-air|to-air] <100-1000000>`

to-air <100-1000000>	Sets the rate limit in the downlink direction, from the network to the wireless client • <100-1000000> – Specify the rate from 100 - 1000000 Kbps.
from-air <100-1000000>	Sets the rate limit in the uplink direction, from the wireless client to the network • <100-1000000> – Specify the rate from 100 - 1000000 Kbps.

Example

```
rfs6000-37FABE(config-radius-group-test)#rate-limit to-air 200

rfs6000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid test
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 rate-limit to-air 200
 policy time start 13:30 end 17:30
rfs6000-37FABE(config-radius-group-test)#
```

Related Commands

no	Removes the RADIUS guest group's rate limits

16.1.4 no

radius-group

Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the `no` command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [guest|policy|rate-limit]


no policy [access|day|inactivity-timeout|role|session-time|ssid|time|vlan]

no policy access [all|console|ssh|telnet|web]
no policy day [all|fr|mo|sa|su|th|tu|we|weekdays]
no policy session-time
no policy ssid [<SSID>|all]
no policy [inactivity-timeout|role|time|vlan]

no rate-limit [from-air|to-air]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or sets its default. Removes or modifies the RADIUS group policy settings. When used in the config RADIUS group mode, the `no` command removes or modifies the following settings: access type, access days, role type, VLAN ID, and SSID.

Example

The following example shows the RADIUS guest group ‘test’ settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-radius-group-test)#show context
radius-group test
 guest
 policy vlan 1
 policy ssid test
 policy day mo
 policy day tu
 policy day we
 policy day th
 policy day fr
 policy day sa
 policy day su
 rate-limit to-air 200
 policy time start 13:30 end 17:30
rfs6000-37FABE(config-radius-group-test)#

rfs6000-37FABE(config-radius-group-test)#no guest
rfs6000-37FABE(config-radius-group-test)#no rate-limit to-air
rfs6000-37FABE(config-radius-group-test)#no policy day all
```

The following example shows the RADIUS guest group ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-radius-group-test)#show context
radius-group test
 policy vlan 1
 policy ssid test
 policy time start 13:30 end 17:30
rfs6000-37FABE(config-radius-group-test)#
```

16.2 radius-server-policy

RADIUS-POLICY

Creates an onboard device RADIUS server policy and enters its configuration mode

A RADIUS server policy is a unique authentication and authorization configuration that receives user connection requests, authenticates users, and returns configuration information necessary for the RADIUS client to deliver service to the user. The client is the entity with authentication information requiring validation. The local RADIUS server has access to a database of authentication information used to validate the client's authentication request.

The local RADIUS server uses authentication schemes like PAP, CHAP, or EAP to verify and confirm information provided by a user. The user's proof of identification is verified, along with, optionally, other information. A local RADIUS server policy can also be configured to refer to an external *Lightweight Directory Access Protocol* (LDAP) resource to verify a user's credentials.

Use the (config) instance to configure RADIUS-Server-Policy related parameters. To navigate to the RADIUS-Server-Policy instance, use the following commands:

```
<DEVICE>(config)#radius-server-policy <POLICY-NAME>

rfs6000-37FABE(config)#radius-server-policy test
rfs6000-37FABE(config-radius-server-policy-test)#?
Radius Configuration commands:
  authentication           Radius authentication
  bypass                   Bypass Certificate Revocation List( CRL ) check
  chase-referral           Enable chasing referrals from LDAP server
  crl-check                Enable Certificate Revocation List( CRL ) check
  ldap-agent               LDAP Agent configuration parameters
  ldap-group-verification  Enable LDAP Group Verification setting
  ldap-server              LDAP server parameters
  local                    RADIUS local realm
  nas                      RADIUS client
  no                       Negate a command or set its defaults
  proxy                    RADIUS proxy server
  session-resumption       Enable session resumption/fast reauthentication by
                           using cached attributes
  termination              Enable Eap termination for proxy requests
  use                      Set setting to use

  clrscr                   Clears the display screen
  commit                   Commit all changes made in this session
  do                       Run commands from Exec mode
  end                      End current mode and change to EXEC mode
  exit                     End current mode and down to previous mode
  help                     Description of the interactive help system
  revert                   Revert changes
  service                  Service Commands
  show                     Show running system information
  write                    Write running configuration to memory or terminal

rfs6000-37FABE(config-radius-server-policy-test)#
```

The following table summarizes RADIUS server policy configuration commands:

Table 16.2 *RADIUS-Server-Policy-Config Commands*

Commands	Description	Reference
authentication	Configures RADIUS authentication settings	*page 16-14*
bypass	Enables bypassing of CRL check	*page 16-16*
chase-referral	Enables LDAP server referral chasing	*page 16-17*
crl-check	Enables a *certificate revocation list* (CRL) check	*page 16-18*
ldap-agent	Configures the LDAP agent's settings	*page 16-19*
ldap-group-verification	Enables LDAP group verification	*page 16-21*
ldap-server	Configures the LDAP server's settings	*page 16-22*
local	Configures a local RADIUS realm	*page 16-25*
nas	Configures the key sent to a RADIUS client	*page 16-26*
no	Removes or resets the RADIUS server policy's settings	*page 16-28*
proxy	Configures the RADIUS proxy server's settings	*page 16-30*
session-resumption	Enables session resumption	*page 16-32*
termination	Enables EAP termination on this current RADIUS server policy. When enabled, EAP authentication is terminated at the controller level.	*page 16-33*
use	Defines settings used with the RADIUS server policy	*page 16-34*

16.2.1 authentication

radius-server-policy

Specifies the RADIUS datasource used for user authentication. Options include local for the local user database or LDAP for a remote LDAP resource.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
authentication [data-source|eap-auth-type]

authentication data-source [ldap|local]
authentication data-source [ldap {fallack}|local] {(ssid <SSID> precedence <1-5000>)}

authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-mschapv2|ttls-pap]
```

Parameters

```
• authentication data-source [ldap {fallback}|local] {(ssid <SSID> precedence <1-5000>)}
```

data-source	The RADIUS sever can either use the local database or an external LDAP server to authenticate a user. It is necessary to specify the data source. The options are: LDAP and local.
ldap fallback	Uses a remote LDAP server as the data source • fallback – Optional. Enables fallback to local authentication. This feature ensures that if the designated external LDAP resource were to fail or become unavailable, the client is authenticated against the local RADIUS resource. This option is disabled by default. When using LDAP as the authentication external source, PEAP-MSCHAPv2 authentication type can be used only if the LDAP server returns the password as plain-text. PEAP-MSCHAPv2 authentication is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory server.
local	Uses the local user database to authenticate a user. This is the default setting.
ssid <SSID> precedence <1-5000>	The following keywords are recursive and common to both 'ldap' and 'local' parameters: • ssid – Optional. Associates the data source, selected in the previous step, with a SSID • <SSID> – Specify the SSID for this authentication data source. The SSID is case sensitive and should not exceed 32 characters in length. Do not use any of the following characters (< > | " & \ ? ,). Contd..

	• precedence <SSID> – Sets the precedence for this authentication rule. The precedence value allows systematic evaluation and application of rules. Rules with the lowest precedence receive the highest priority. • <1-5000> – Specify a precedence from 1- 5000. Specifying the SSID allows the RADIUS server to use the SSID attribute in access requests to determine the data source to use. This option is applicable to onboard RADIUS servers only.

```
• authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|ttls-
mschapv2|ttls-pap]
```

eap-auth-type	Uses *Extensible Authentication Protocol* (EAP), with this RADIUS server policy, for user authentication The EAP authentication types supported by the local RADIUS server are: all, peap-gtc, peap-mschapv2, tls, ttls-md5, ttls-mschapv2, ttls-pap.
all	Enables both TTLS and PEAP authentication. This is the default setting.
peap-gtc	Enables PEAP with default authentication using GTC
peap-mschapv2	Enables PEAP with default authentication using MSCHAPv2 When using LDAP as the authentication external source, PEAP-MSCHAPv2 authentication type can be used only if the LDAP server returns the password as plain-text. PEAP-MSCHAPv2 authentication is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory server.
tls	Enables TLS as the EAP type
ttls-md5	Enables TTLS with default authentication using md5
ttls-mschapv2	Enables TTLS with default authentication using MSCHAPv2
ttls-pap	Enables TTLS with default authentication using PAP

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#authentication eap-auth-type tls

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Removes the RADIUS authentication settings

16.2.2 bypass

radius-server-policy

Enables bypassing a CRL check. When enabled, this feature bypasses checks for missing and expired CRLs. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
bypass [crl-check|expired-crl]
```

Parameters

- `bypass [crl-check|expired-crl]`

bypass [crl-check|expired-crl]	Bypasses CRL check based on the parameters passed • crl-check – Bypasses CRL check of missing CRLs • expired-crl – Bypasses CRL check of expired CRLs **Note:** A CRL is a list of certificates that have been revoked or are no longer valid.

Example

```
nx9500-6C8809(config-radius-server-policy-test)#bypass crl-check

nx9500-6C8809(config-radius-server-policy-test)#no bypass crl-check

nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 no bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands

no	Disables bypassing of checking for missing CRLs or expired CRLs

16.2.3 chase-referral

radius-server-policy

Enables chasing of referrals from an external LDAP server resource

An LDAP referral is a controller or service platform's way of indicating to a client it does not hold the section of the directory tree where a requested content object resides. The referral is the controller or service platform's direction to the client a different location is more likely to hold the object, which the client uses as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the domain controller to generate another referral, although it usually does not take long to discover the object does not exist and inform the client.

This feature is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
chase-referral
```

Parameters

None

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#chase-referral
```

Related Commands

no	Disables LDAP server referral chasing

16.2.4 crl-check

radius-server-policy

Enables a *certificate revocation list* (CRL) check on this RADIUS server policy

A CRL is a list of revoked certificates issued and subsequently revoked by a *Certification Authority* (CA). Certificates can be revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. The mechanism used for certificate revocation depends on the CA.

This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
crl-check
```

Parameters

None

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#crl-check

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Disables CRL check on a RADIUS server policy

16.2.5 ldap-agent

radius-server-policy

Configures the LDAP agent's settings in the RADIUS server policy context

When a user's credentials are stored on an external LDAP server, the local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource (using credentials maintained locally).

This feature is available to all controller, service platforms and access point models, with the exception of AP6511 and AP6521 models running in standalone AP or virtual controller AP mode. However, this feature is supported by dependent mode AP6511 and AP6521 model access points when adopted and managed by a controller or service platform.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-agent [join|join-retry-timeout|primary|secondary]

ldap-agent [join {on <DEVICE-NAME>}|join-retry-timeout <60-300>]

ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME> domain-admin-user
<ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

Parameters

- `ldap-agent [join {on <DEVICE-NAME>}|join-retry-timeout <60-300>]`

ldap-agent	Configures the LDAP agent's settings
join {on <DEVICE-NAME>}	Initiates the join process, which binds the RADIUS server with the LDAP server's (Windows) domain. When successful, the hostname (name of the AP, wireless controller, or service platform) is added to the LDAP server's Active Directory. • on <DEVICE-NAME> – Optional. Specifies the device name • <DEVICE-NAME> – Specify the name of the AP, wireless controller, or service platform. To confirm the join status of a controller, use the *show > ldap-agent > join-status* command.
join-retry-timeout <60-300>	If the join process fails (i.e. the RADIUS server fails to join the LADP server's domain), the process is retried after a specified interval. This command configures the interval (in seconds) between two successive join attempts. • <60-300> – Set the timeout value from 60 - 300 seconds. The default is 60 seconds. A retry timer is initiated as soon as the join process starts, which tracks the time lapse in case of a failure.

```
• ldap-agent [primary|secondary] domain-name <LDAP-DOMAIN-NAME> domain-admin-user
<ADMIN-USER-NAME> domain-admin-password [0 <WORD>|2 <WORD>]
```

ldap-agent	Configures the LDAP agent's settings
primary	Configures the primary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the primary LDAP server.
secondary	Configures the secondary LDAP server details, such as domain name, user name, and password. The RADIUS server uses these credentials to bind with the secondary LDAP server.
domain-name <LDAP-DOMAIN-NAME>	This keyword is common to both the 'primary' and 'secondary' parameters. • domain-name – Configures the primary or secondary LDAP server's domain name • <LDAP-DOMAIN-NAME> – Specify the domain name.
domain-admin-user <ADMIN-USER-NAME>	This keyword is common to both the 'primary' and 'secondary' parameters. • domain-admin-user – Configures the primary or secondary LDAP server's admin user name • <ADMIN-USER-NAME> – Specify the admin user's name.

domain-admin-password [0 <WORD>| 2 <WORD>]	This keyword is common to both the 'primary' and 'secondary' parameters.
	• domain-admin-password – Configures the primary or secondary LDAP server's admin user password
	  • 0 <WORD> – Specifies the password in the unencrypted format
	  • 2 <WORD> – Specifies the password in the encrypted format

Example

```
rfs4000-229D58(config-radius-server-policy-test)#ldap-agent primary domain-name
test domain-admin-user Administrator domain-admin-password 0 test@123
rfs4000-229D58(config-radius-server-policy-test)#

rfs4000-229D58(config-radius-server-policy-test)#show context
radius-server-policy test
 ldap-agent primary domain-name test domain-admin-user Administrator domain-admin-
password 0 test@123
rfs4000-229D58(config-radius-server-policy-test)#
```

Related Commands

no	Removes LDAP agent settings from this RADIUS server policy

16.2.6 ldap-group-verification

radius-server-policy

Enables LDAP group verification settings on this RADIUS server policy. This option is enabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-group-verification
```

Parameters

None

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#ldap-group-verification
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Disables LDAP group verification settings

16.2.7 ldap-server

radius-server-policy

Configures the LDAP server's settings. Configuring LDAP server allows users to login and authenticate from anywhere on the network.

Administrators have the option of using the local RADIUS server to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative user management overhead making RADIUS authorization more secure and efficient.

RADIUS is not just a database. It is a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the local RADIUS server to free up resources and manage user credentials from a secure remote location. It is the local RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. A LDAP user database alone cannot perform such complex authorization checks.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-server [dead-period|primary|secondary]

ldap-server dead-period <0-600>

ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME> bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>] passwd-attr <ATTR> group-attr <ATTR> group-filter <FILTER> group-membership <WORD> {net-timeout <1-10>|start-tls net-timeout <1-10>|tls-mode net-timeout <1-10>}
```

Parameters

- `ldap-server dead-period <0-600>`

dead-period <0-600>	Sets an interval, in seconds, during which the local server will not contact its LDAP server resource once its been defined as unavailable. A dead period is only implemented when additional LDAP servers are configured and available. • <0-600> – Specify a value from 0 - 600 seconds. The default is 300 seconds.

- `ldap-server [primary|secondary] host <IP> port <1-65535> login <LOGIN-NAME> bind-dn <BIND-DN> base-dn <BASE-DN> passwd [0 <PASSWORD>|2 <ENCRYPTED-PASSWORD>|<PASSWORD>] passwd-attr <ATTR> group-attr <ATTR> group-filter <FILTER> group-membership <WORD> {net-timeout <1-10>|start-tls net-timeout <1-10>|tls-mode net-timeout <1-10>}}`

ldap primary	Configures the primary LDAP server settings
ldap secondary	Configures the secondary LDAP server settings
host <IP>	Specifies the LDAP host's IP address • <IP> – Specify the LDAP server's IP address.

port <1-65535>	Configures the LDAP server port • <1-65535> – Specify a port between 1 - 65535.
login <LOGIN-NAME>	Configures the login name of a user to access the LDAP server • <LOGIN-NAME> – Specify a login ID (should not exceed 127 characters).
bind-dn <BIND-DN>	Configures a distinguished bind name. This is the *distinguished name* (DN) used to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas. • <BIND-DN> – Specify a bind name (should not exceed 127 characters).
base-dn <BASE-DN>	Configures a distinguished base name. This is the DN that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with a specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the *Relative Distinguished Name* (RDN). It identifies an entry distinctly from any other entries that have the same parent • <BASE-DN> – Specify a base name (should not exceed 127 characters).
passwd [0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Sets a valid password for the LDAP server. • 0 <PASSWORD> – Sets an UNENCRYPTED password • 2 <ENCRYPTED-PASSWORD> – Sets an ENCRYPTED password • <PASSWORD> – Sets the LDAP server bind password, specified UNENCRYPTED, with a maximum size of 31 characters
passwd-attr <ATTR>	Specify the LDAP server password attribute (should not exceed 63 characters).
group-attr <ATTR>	Specify a name to configure group attributes (should not exceed 31 characters). LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name.
group-filter <FILTER>	Specify a name for the group filter attribute (should not exceed 255 characters). This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.
group-membership <WORD>	Specify a name for the group membership attribute (should not exceed 63 characters). This attribute is sent to the LDAP server when authenticating users.
net-time <1-10>	Optional. Select a value from 1 - 10 to configure the network timeout (number of seconds to wait for a response from the target primary or secondary LDAP server). The default is 10 seconds.
start-tls net-timeout <1-10>	Optional. Select a value from 1 - 10 to configure the network timeout for secure communication using start_tls support on the external LDAP server.
tls-mode net-timeout <1-10>	Optional. Select a value from 1 - 10 to configure the network timeout for secure communication using tls_mode support on the external LDAP server.

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#ldap-server dead-period 100

rfs6000-37FABE(config-radius-server-policy-test)#ldap-server primary host 172.16
.10.19 port 162 login test bind-dn bind-dn1 base-dn base-dn1 passwd 0 test@123
passwd-attr test123 group-attr group1 group-filter groupfilter1
group-membership groupmembership1 net-timeout 2
rfs6000-37FABE(config-radius-server-policy-test)#

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Disables the LDAP server parameters

16.2.8 local

radius-server-policy

Configures a local RADIUS realm on this RADIUS server policy

When the local RADIUS server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
local realm <RADIUS-REALM>
```

Parameters

- `local realm <RADIUS-REALM>`

realm <RADIUS-REALM>	Configures a local RADIUS realm • <RADIUS-REALM> – Sets a local RADIUS realm name (a string not exceeding 50 characters)

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#local realm realm1

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Removes the RADIUS local realm

16.2.9 nas

radius-server-policy

Configures the key sent to a RADIUS client

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or Access Point managed network.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash algorithm to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified access reject message, the username and password are considered to be incorrect, and the user is not authenticated.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
nas <IP/M> secret [0|2|<LINE>]

nas <IP/M> secret [0 <LINE>|2 <LINE>|<LINE>]
```

Parameters

```
• nas <IP/M> secret [0 <LINE>|2<LINE>]
```

<IP/M>	Sets the RADIUS client's IP address • <IP/M> – Sets the RADIUS client's IP address in the A.B.C.D/M format
secret [0 <LINE>|2 <LINE>| <LINE>]	Sets the RADIUS client's shared secret. Use one of the following options: • 0 <LINE> – Sets an UNENCRYPTED secret • 2 <LINE> – Sets an ENCRYPTED secret • <LINE> – Defines the secret (client shared secret) up to 64 characters

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#nas 172.16.10.10/24 secret 0
wirelesswell

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 nas 172.16.10.10/24 secret 0 wirelesswell
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "base-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
 ldap-server dead-period 100
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Removes a RADIUS server's client on a RADIUS server policy

16.2.10 no

radius-server-policy

Negates a command or reverts back to default settings. When used with in the config RADIUS server policy mode, the no command removes settings, such as crl-check, LDAP group verification, RADIUS client, etc.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [authentication|bypass|chase-referral|clr-check|ldap-agent|ldap-group-
verification|ldap-server|local|nas|proxy|session-resumption|termination|use]

no bypass [crl-check|expired-crl]

no authentication [data-source|eap]

no authentication [data-source {ldap {fallback}|local|ssid}|eap configuration]

no [chase-referral|clr-check|ldap-group-verification|nas <IP/M>|session-
resumption]

no ldap-agent [join-retry-timeout|primary|secondary]

no local realm [<REALM-NAME>|all]

no proxy [realm <REALM-NAME>|retry-count|retry-delay]

no ldap-server [dead-period|primary|secondary]

no termination

no use [radius-group [<RAD-GROUP-NAME>|all]|radius-user-pool-policy [<RAD-USER-
POOL-NAME>|all]]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates a command or reverts back to default settings. When used with in the config RADIUS server policy mode, the no command removes settings, such as crl-check, LDAP group verification, RADIUS client etc

Example

The following example shows the RADIUS server policy 'test' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 authentication eap-auth-type tls
 crl-check
 nas 172.16.10.10/24 secret 0 wirelesswell
 local realm realm1
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
 ldap-server dead-period 100
```

```
rfs6000-37FABE(config-radius-server-policy-test)#

rfs6000-37FABE(config-radius-server-policy-test)#no authentication eap
configuration
rfs6000-37FABE(config-radius-server-policy-test)#no crl-check
rfs6000-37FABE(config-radius-server-policy-test)#no local realm realm1
rfs6000-37FABE(config-radius-server-policy-test)#no nas 172.16.10.10/24
rfs6000-37FABE(config-radius-server-policy-test)#no ldap-server dead-period
```

The following example shows the RADIUS server policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
rfs6000-37FABE(config-radius-server-policy-test)#
```

16.2.11 proxy

radius-server-policy

Configures a proxy RADIUS server based on the realm/suffix. The realm identifies where the RADIUS server forwards AAA requests for processing.

A user's access request is sent to a proxy RADIUS server if it cannot be authenticated by the local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the proxy server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
proxy [realm|retry-count|retry-delay]

proxy realm <REALM-NAME> server <IP> port <1024-65535> secret [0 <PASSWORD>|2
<ENCRYPTED-PASSWORD>|<PASSWORD>]

proxy retry-count <3-6>

proxy retry-delay <5-10>
```

Parameters

```
• proxy realm <REALM-NAME> server <IP> port <1024-65535> secret [0 <PASSWORD>|2
<ENCRYPTED-PASSWORD>|<PASSWORD>]
```

proxy realm <REALM-NAME>	Configures the realm name • <REALM-NAME> – Specify the realm name. The name should not exceed 50 characters.
server <IP>	Configures the proxy server's IP address. This is the address of server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server. • <IP> – Sets the proxy server's IP address
port <1024-65535>	Configures the proxy server's port. This is the TCP/IP port number for the server that acts as a data source for the proxy server. • <1024-65535> – Sets the proxy server's port from 1024 - 65535 (default port is 1812)
secret [0 <PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>	Sets the proxy server secret string. The options are: • 0 <PASSWORD> – Sets an UNENCRYPTED password • 2 <ENCRYPTED-PASSWORD> – Sets an ENCRYPTED password • <PASSWORD> – Sets the proxy server shared secret value

- `proxy retry-count <3-6>`

retry-count <3-6>	Sets the proxy server's retry count. This is the maximum number attempts made by a controllers RADIUS server to connect to the proxy server. • <3-6> – Sets a value from 3 - 6 (default is 3 counts)

- `proxy retry-delay <5-10>`

retry-delay <5-10>	Sets the proxy server's retry delay count. This is the interval the controller's RADIUS server waits before making an additional connection attempt. • <5-10> – Sets a value from 5 - 10 seconds (default is 5 seconds)

Usage Guidelines

A maximum of five RADIUS proxy servers can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times RADIUS requests are transmitted before giving up. The timeout value is the defines the interval between successive retransmission of a RADIUS request (in case of no reply).

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#proxy realm test1 server 172.16
.10.7 port 1025 secret 0 test1123

rfs6000-37FABE(config-radius-server-policy-test)#proxy retry-count 4

rfs6000-37FABE(config-radius-server-policy-test)#proxy retry-delay 8

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Removes or resets the RADIUS proxy server's settings

16.2.12 session-resumption

radius-server-policy

Enables session resumption or fast re-authentication by using cached attributes. This feature controls the volume and duration cached data is maintained by the server policy, upon termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption.

This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
session-resumption {lifetime|max-entries}

session-resumption {lifetime <1-24> {max-entries <10-1024>}|max-entries <10-1024>}
```

Parameters

- `session-resumption {lifetime <1-24> {max-entries <10-1024>}|max-entries <10-1024>}`

lifetime <1-24> {max-entries <10-1024>}	Optional. Sets the lifetime of cached entries • <1-24> – Specify the lifetime period from 1 - 24 hours (default is 1 hour) • max-entries – Optional. Configures the maximum number of entries in the cache • <10-1024> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)
max-entries <10-1024>	Optional. Configures the maximum number of entries in the cache • <10-1024> – Sets the maximum number of entries in the cache from 10 - 1024 (default is 128 entries)

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#session-resumption lifetime 10
max-entries 11

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
 session-resumption lifetime 10 max-entries 11
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Disables session resumption on this RADIUS server policy

16.2.13 termination

radius-server-policy

Enables EAP termination on this RADIUS server policy. When enabled, EAP authentication is terminated at the controller level. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
termination
```

Parameters

None

Example

```
nx9500-6C8809(config-radius-server-policy-test)#termination

nx9500-6C8809(config-radius-server-policy-test)#show context
radius-server-policy test
 termination
 no bypass crl-check
nx9500-6C8809(config-radius-server-policy-test)#
```

Related Commands

no	Disables EAP termination on this RADIUS server policy

16.2.14 use

radius-server-policy

Defines settings used with the RADIUS server policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}|radius-user-pool-policy
  <RAD-USER-POOL-NAME>]
```

Parameters

```
• use [radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}|radius-user-pool-policy
<RAD-USER-POOL-NAME>]
```

radius-group <RAD-GROUP-NAME1> {RAD-GROUP-NAME2}	Associates a specified RADIUS group (for LDAP users) with this RADIUS server policy You can optionally associate two RADIUS groups with one RADIUS server policy.
radius-user-pool-policy <RAD-USER-POOL-NAME>	Associates a specified RADIUS user pool with this RADIUS server policy. Specify a user pool name.

Example

```
rfs6000-37FABE(config-radius-server-policy-test)#use radius-group test

rfs6000-37FABE(config-radius-server-policy-test)#show context
radius-server-policy test
 proxy retry-delay 8
 proxy retry-count 4
 proxy realm test1 server 172.16.10.7 port 1025 secret 0 test1123
 ldap-server primary host 172.16.10.19 port 162 login "test" bind-dn "bind-dn1"
base-dn "bas-dn1" passwd 0 test@123 passwd-attr test123 group-attr group1 group-
filter "groupfilter1" group-membership groupmembership1 net-timeout 2
 use radius-group test
 session-resumption lifetime 10 max-entries 11
rfs6000-37FABE(config-radius-server-policy-test)#
```

Related Commands

no	Disassociates a RADIUS group or a RADIUS user pool policy from this RADIUS server policy

16.3 radius-user-pool-policy

RADIUS-POLICY

Configures a RADIUS user pool policy and enters its configuration mode

A user pool defines policies for individual user access to the internal RADIUS resources. User pool policies define unique permissions (either temporary or permanent) that control user access to the local RADIUS resources. A pool can contain a single user or multiple users.

Use the (config) instance to configure RADIUS user pool policy commands. To navigate to the radius-user-pool-policy instance, use the following commands:

```
<DEVICE>(config)#radius-user-pool-policy <POOL-NAME>

rfs6000-37FABE(config)#radius-user-pool-policy testuser
rfs6000-37FABE(config-radius-user-pool-testuser)#

rfs6000-37FABE(config-radius-user-pool-testuser)#?
Radius User Pool Mode commands:
  duration  Set a guest user's access duration
  no        Negate a command or set its defaults
  user      Radius user configuration

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

rfs6000-37FABE(config-radius-user-pool-testuser)#
```

The following table summarizes RADIUS user pool policy configuration commands:

Table 16.3 *RADIUS-User-Pool-Policy-Config Commands*

Commands	Description	Reference
duration	Modifies a guest user's duration of captive-portal access	*page 16-36*
user	Configures the RADIUS user parameters	*page 16-37*
no	Negates a command or sets its default	*page 16-40*

16.3.1 duration

radius-user-pool-policy

Modifies the duration, in minutes, that a guest user can access the captive portal

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
duration <GUEST-USER-NAME> <0-525600>
```

Parameters

- `duration <GUEST-USER-NAME> <0-525600>`

duration <GUEST-USER-NAME> <0-525600>	Modifies the duration of captive-portal access (in minutes) for the guest user identified by the <GUEST-USER-NAME> keyword • <GUEST-USER-NAME> – Specify the guest user's name. • <0-525600> – Specify the access duration from 0 - 525600 minutes. A value of "0" indicates unlimited access. The default is 1440 minutes.

Example

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-
date 12/15/2014 access-duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#

rfs4000-229D58(config-radius-user-pool-wdws)#duration guestuser1 200

rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-
date 12/15/2014 access-duration 200
rfs4000-229D58(config-radius-user-pool-wdws)#
```

16.3.2 user

radius-user-pool-policy

Configures RADIUS user parameters

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>] {group <RAD-GROUP-NAME>} {guest}

user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-
PASSWORD>|<PASSWORD>] {group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-
date <MM/DD/YYYY> {access-duration <0-525600>|data-limit|email-id <EMAIL-ID>|
start-time <HH:MM> start-date <MM/DD/YYY>|telephone <TELEPHONE-NUMBER>}}

user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>] {group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date <MM/
DD/YYYY> {access-duration <0-525600>|data-limit <1-102400> committed-downlink
<100-1000000> committed-uplink <100-1000000> reduced-downlink <100-1000000>
reduced-uplink <100-1000000>|email-id <EMAIL-ID>|start-time <HH:MM> start-date
<MM/DD/YYY>|telephone <TELEPHONE-NUMBER>}}
```

Parameters

```
• user <USERNAME> password [0 <UNECRYPTED-PASSWORD>|2 <ENCRYPTED-PASSWORD>|
<PASSWORD>] {group <RAD-GROUP-NAME>} {guest expiry-time <HH:MM> expiry-date
<MM:DD:YYY> {access-duration <0-525600>|data-limit <1-102400> committed-downlink
<100-1000000>   committed-uplink <100-1000000> reduced-downlink <100-1000000>
reduced-uplink <100-1000000>|email-id <EMAIL-ID>|start-time <HH:MM> start-date
<MM/DD/YYY>|telephone <TELEPHONE-NUMBER>}}
```

user <USERNAME>	Adds a new RADIUS user to the RADIUS user pool • <USERNAME> – Specify the name of the user. The username should not exceed 64 characters. **Note:** The username is a unique alphanumeric string identifying this user, and cannot be modified with the rest of the configuration.
passwd [0 <UNENCRYPTED-PASSWORD>| 2 <ENCRYPTED-PASSWORD>| <PASSWORD>]	Configures the user password (provide a password unique to this user) • 0 <UNENCRYPTED-PASSWORD> – Sets an unencrypted password • 2 <ENCRYPTED-PASSWORD> – Sets an encrypted password • <PASSWORD> – Sets a password (specified unencrypted) up to 21 characters
group <RAD-GROUP-NAME>	Optional. Configures the RADIUS server group of which this user is a member • <RAD-GROUP-NAME> – Specify the group name in the local database. If the user is a guest, assign the user a group with temporary access privileges.
guest	Optional. Specifies that this user is a guest user. Guest users have restricted access. After enabling a guest user account, specify the expiry time and date for this account. A guest user can be assigned only to a guest user group.

expiry-time <HH:MM>	Specify the user account expiry time in the HH:MM format (for example, 12:30 means 30 minutes after 12:00 the user login will expire).
expiry-date <MM:DD:YYYY>	Specify the user account expiry date in the MM:DD:YYYY format (for example. 02:15:2014).
{access-duration <0-525600>|data-limit <1-102400> committed-downlink <100-1000000> committed-uplink <100-1000000> reduced-downlink <100-1000000> reduced-uplink <100-1000000>| email-id <EMAIL-ID>| start-time <HH:MM> start-date <MM:DD:YYY>| telephone <TELEPHONE-NUMBER>}	After configuring the above user details, optionally configure the following user information: • access-duration <0-525600> – Configures the duration, in minutes, for which this guest user can access the captive portal. • <0-525600> – Specify a value from 0 - 525600 minutes. • data-limit <1-102400> – Configures the data limit for which this guest user can access the captive portal. Specify a value from 1 - 102400 bytes. • committed-downlink <100-1000000> – Configures committed downlink bandwidth until data limit is reached. This value represents the download speed (in kilobits per second) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the *reduced downlink rate* (specified using this command). Specify a value from 100 - 1000000 Kbps. • committed-uplink <100-1000000> – Configures committed uplink bandwidth until data limit is reached. This value represents the upload speed (in kilobits per second) allocated to the guest user. When bandwidth is available, the user can upload data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the *reduced uplink rate* (specified using this command). Specify a value from 100 - 1000000 Kbps. • reduced-downlink <100-1000000> – Configures reduced downlink bandwidth after data Limit is reached. This value represents the reduced speed the guest utilizes (in kilobits per second) when exceeding the specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the *reduced downlink rate* specified here. Specify a value from 100-1000000 Kbps. • reduced-uplink <100-1000000> – Configures reduced uplink bandwidth after data Limit is reached. This value represents the reduced speed the guest utilizes (in kilobits per second) when exceeding the specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified data limit, the speed is throttled to the *reduced uplink rate* specified here. Specify a value from 100 - 1000000 Kbps. • email-id – Optional. User's e-mail ID • start-time – Optional. User's account activation time. After specifying the activation time, specify the activation date. • start-date – User's account activation date • telephone – Optional. User's telephone number (should include the area code) Contd..

	To view access details of guest users on a RADIUS server, in the Priv Executable Configuration mode, use the following command:
	show > radius > guest-users
	`rfs6000-37FABE#show radius guest-users time`
	`TIME (min:sec)`
	`USED REMAINING GUEST USER`
	`0:00 500:00 user1`
	`Current time: 09:03:07`
	`rfs6000-37FABE#`

Example

```
rfs4000-229D58(config-radius-user-pool-wdws)#user guestuser1 password 0
guestuser@1 group wdws guest expiry-time 12:30 expiry-date 12/15/2014 access-
duration 500
rfs4000-229D58(config-radius-user-pool-wdws)#

rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-
date 12/15/2014 access-duration  500
rfs4000-229D58(config-radius-user-pool-wdws)#

nx4500-5CFA2B(config-radius-user-pool-pool1)#user word password 0 word group gro
up1 guest expiry-time 11:10 expiry-date 12/12/2014 data-limit 10 committed-downl
ink 103 committed-uplink 100 reduced-downlink 102 reduced-uplink 101
nx4500-5CFA2B(config-radius-user-pool-pool1)#
```

Related Commands

no	Deletes a user from a RADIUS user pool

16.3.3 no

radius-user-pool-policy

Negates a command or sets its default. When used in the RADIUS user pool policy mode, the `no` command deletes a user from a RADIUS user pool

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no user <USERNAME>
```

Parameters

- `no user <USERNAME>`

no user <USERNAME>	Deletes a RADIUS user • <USERNAME> – Specify the user name.

Example

The following example shows the RADIUS user pool 'wdws' settings before the 'no' command is executed:

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
 user guestuser1 password 0 guestuser@1 group wdws guest expiry-time 12:30 expiry-
date 12/15/2014 access-duration  500
rfs4000-229D58(config-radius-user-pool-wdws)#

rfs4000-229D58(config-radius-user-pool-wdws)#no user guestuser1
```

The following example shows the RADIUS user pool 'wdws' settings after the 'no' command is executed:

```
rfs4000-229D58(config-radius-user-pool-wdws)#show context
radius-user-pool-policy wdws
rfs4000-229D58(config-radius-user-pool-wdws)#
```

Related Commands

user	Configures the RADIUS user parameters

17 RADIO-QOS-POLICY

This chapter summarizes the radio QoS policy in the CLI command structure.

Configuring and implementing a radio QoS policy is essential for WLANs with heavy traffic and less bandwidth. The policy enables you to provide preferential service to selected network traffic by controlling bandwidth allocation. The radio QoS policy can be applied to VLANs configured on an access point. In case no VLANs are configured, the radio QoS policy can be applied to an access point's Ethernet and radio ports.

Without a dedicated QoS policy, a network operates on a best-effort delivery basis, meaning all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy's intended wireless client base.

A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy.

Within a managed wireless network, wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined *Enhanced Distributed Channel Access* (EDCA) mechanisms stating high priority traffic can access the network sooner then lower priority traffic. The EDCA defines four traffic classes (or access categories); voice (highest), video (next highest), best effort, and background (lowest). The EDCA has defined a time interval for each traffic class, known as the *Transmit Opportunity* (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported.

IEEE 802.11e includes an advanced power saving technique called *Unscheduled Automatic Power Save Delivery* (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an access point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an access point. U-APSD also allows access points to deliver buffered data frames as *bursts*, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. A managed wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must also support WMM and use the values correctly while accessing the WLAN to benefit.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected access point radios and their wireless clients. Parameters impacting access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

Wireless network controllers (access points, controllers, and service platforms) include a *Session Initiation Protocol* (SIP), *Skinny Call Control Protocol* (SCCP) and *Application Layer Gateway* (ALG) enabling devices to identify voice streams and dynamically set voice call bandwidth.

Wireless network controllers also support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN's WMM access control setting.

NOTE: Statistically setting a WLAN WMM access category value only prioritizes traffic to the client.

Wireless network administrators can also assign weights to each WLAN in relation to user priority levels. The lower the weight, the lower the priority. Use a weighted technique to achieve different QoS levels across WLANs.

All devices rate-limit bandwidth for WLAN sessions. This form of per-user rate limiting enables administrators to define uplink and downlink bandwidth limits for users and clients. This sets the level of traffic a user or client can forward and receive over the WLAN. If the user or client exceeds the limit, excessive traffic is dropped. Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using *Vendor Specific Attributes* (VSAs). Rate limits can be applied to users authenticating using 802.1X, captive portal authentication, and devices using MAC authentication.

Use the (config) instance to configure radios QoS policy related configuration commands. To navigate to the radio QoS policy instance, use the following commands:

```
<DEVICE>(config)#radio-qos-policy <POLICY-NAME>

rfs6000-37FABE(config)#radio-qos-policy test
rfs6000-37FABE(config-radio-qos-test)#?
Radio QoS Mode commands:
  accelerated-multicast  Configure multicast streams for acceleration
  admission-control      Configure admission-control on this radio for one or
                         more access categories
  no                     Negate a command or set its defaults
  smart-aggregation      Configure smart aggregation parameters
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs6000-37FABE(config-radio-qos-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

17.1 radio-qos-policy

- *RADIO-QOS-POLICY*

The following table summarizes radio QoS policy configuration commands:

Table 17.1 *Radio-QoS-Policy-Config Commands*

Command	Description	Reference
accelerated-multicast	Configures multicast streams for acceleration	*page 17-5*
admission-control	Enables admission control across all radios for one or more access categories	*page 17-6*
no	Negates a command or resets configured settings to their default	*page 17-10*
smart-aggregation	Configures smart aggregation parameters	*page 17-12*
service	Invokes service commands in the radio QoS configuration mode	*page 17-14*
wmm	Configures 802.11e/wireless multimedia parameters	*page 17-16*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

17.1.1 accelerated-multicast

radio-qos-policy

Configures multicast streams for acceleration. Multicasting allows group transmission of data streams.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
accelerated-multicast [client-timeout|max-client-streams|max-streams|overflow-policy|stream-threshold]

accelerated-multicast [client-timeout <5-6000>|max-client-streams <1-4>|max-streams <0-256>|overflow-policy [reject|revert]|stream-threshold <1-500>]
```

Parameters

```
• accelerated-multicast [client-timeout <5-6000>|max-client-streams <1-4>|max-streams <0-256>|overflow-policy [reject|revert]|stream-threshold <1-500>]
```

client-timeout <5-6000>	Configures a timeout period in seconds for wireless clients • <5-6000> – Specify a value from 5 - 6000 seconds. The default is 60 seconds.
max-client-streams <1-4>	Configures the maximum number of accelerated multicast streams per client • <1-4> – Specify a value from 1 - 4. The default is 2.
max-streams <0-256>	Configures the maximum number of accelerated multicast streams per radio • <0-256> – Specify a value from 0 - 256. The default is 25.
overflow-policy [reject|revert]	Specifies the policy in case too many clients register simultaneously. The radio QOS policy can be configured to follow one of the following courses of action: • reject – Rejects new clients. The default overflow policy is reject. • revert – Reverts to regular multicast delivery When the number of wireless clients using accelerated multicast exceeds the configured value (max-streams), the radio can either reject new wireless clients or revert existing clients to a non-accelerated state.
stream-threshold <1-500>	Configures the number of multicast packets per second threshold value. Once this threshold is crossed, the system triggers streams to accelerate. • <1-500> – Specify a value from 1 - 500. The default is 25 packets per second.

Example

```
rfs6000-37FABE(config-radio-qos-test)#accelerated-multicast client-timeout 500
rfs6000-37FABE(config-radio-qos-test)#accelerated-multicast stream-threshold 15

rfs6000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
rfs6000-37FABE(config-radio-qos-test)#
```

Related Commands

no	Reverts accelerated multicasting settings to their default

17.1.2 admission-control

radio-qos-policy

Enables admission control across all radios for one or more access categories. Enabling admission control for an access category, ensures clients associated to an access point and complete WMM admission control before using that access category.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
admission-control [background|best-effort|firewall-detected-traffic|implicit-tspec|video|voice]

admission-control [firewall-detected-traffic|implicit-tspec]

admission-control [background|best-effort|video|voice] {max-airtime-percent|max-clients|max-roamed-clients|reserved-for-roam-percent}

admission-control [background|best-effort|video|voice] {max-airtime-percent <0-150>|max-clients <0-256>|max-roamed-clients <0-256>|reserved-for-roam-percent <0-150>}
```

Parameters

- `admission-control [firewall-detected-traffic|implicit-tspec]`

admission-control firewall-detected-traffic	Enforces admission control for traffic whose access category is detected by the firewall ALG. For example, SIP voice calls. This feature is enabled by default. When enabled, the firewall simulates reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TSPEC frames only.
admission-control implicit-tspec	Enables implicit traffic specifiers for clients that do not support WMM TSPEC, but are accessing admission-controlled access categories. This feature is enabled by default. This feature requires wireless clients to send their traffic specifications to an access point before they can transmit or receive data. If enabled, this setting applies to this radio QoS policy. When enabled, the access point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TSPEC frames only.

- `admission-control [background|best-effort|video|voice] {max-airtime-percent <0-150>|max-clients <0-256>|max-roamed-clients <0-256>|reserved-for-roam-percent <0-150>}`

admission-control background	Configures background access category admission control parameters

admission-control best-effort	Configures best effort access category admission control parameters
admission-control video	Configures video access category admission control parameters
admission-control voice	Configures voice access category admission control parameters
max-airtime-percent <0-150>	Optional. Specifies the maximum percentage of airtime, including oversubscription, for the following access category: • background – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for low (background) client traffic. Background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved to support background data. • best-effort – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal (best-effort) client traffic. Normal best effort traffic needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for best effort data support. • video – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video. • voice – Sets the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice. The following keyword is common to all of the above traffic types: • <0-150> – Specify a value from 0 - 150. This is the maximum percentage of air-time, including oversubscription, for the selected access category. The default is 75%.
max-clients <0-256>	Optional. Specifies the maximum number of wireless clients admitted to the following access categories: • background – Sets the number of wireless clients supporting low (background) traffic allowed to exist (and consume bandwidth) within the radio's QoS policy • best-effort – Sets the number of wireless clients supporting normal (best-effort) traffic allowed to exist (and consume bandwidth) within the radio's QoS policy • video – Sets the number of video supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. • voice – Sets the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Since voice and video supported wireless clients use a greater portion of a controller's resources than lower bandwidth traffic (like low and best effort categories), consider setting the max-client value proportionally to the number of other QoS policies supporting voice access category clients. The following keyword is common to all of the above traffic types: • <0-256> – Specify a value from 0 - 256. This is the maximum number of wireless clients admitted to the selected access category. The default is 100 clients.

max-roamed-clients <0-256>	Optional. Specifies the maximum number of roaming wireless clients admitted to the selected access category • background – Sets the number of low (background) supported wireless clients allowed to roam to a different access point radio • best-effort – Sets the number of normal (best-effort) supported wireless clients allowed to roam to a different access point radio • video – Sets the number of video supported wireless clients allowed to roam to a different access point radio • voice – Sets the number of voice supported wireless clients allowed to roam to a different access point radio The following keyword is common to all of the above traffic types: • <0-256> – Specify a value from 0 - 256. This is the maximum number of roaming wireless clients admitted to the selected access category. The default is 10 roamed clients.
reserved-for-roam-percent <0-150>	Optional. Calculates the percentage of air time, including oversubscription, allocated exclusively for roaming clients. This value is calculated relative to the configured max air time for this access category. • background – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for low (background) supported clients who have roamed to a different radio. • best-effort – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal (best-effort) supported clients who have roamed to a different radio. • video – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different radio. • voice – Sets the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio. The following keyword is common to all of the above traffic types: • <0-150> – Specify a value from 0 - 150. This is the percentage of air time, including oversubscription, allocated exclusively for roaming clients associated with the selected access category. The default is 10%.

Example

```
rfs6000-37FABE(config-radio-qos-test)#admission-control best-effort max-clients
200
rfs6000-37FABE(config-radio-qos-test)#admission-control voice reserved-for-roam-
percent 8
rfs6000-37FABE(config-radio-qos-test)#admission-control voice max-airtime-percent
9

rfs6000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 admission-control best-effort max-clients 200
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
rfs6000-37FABE(config-radio-qos-test)#
```

Related Commands

no	Reverts or resets admission control settings to their default

17.1.3 no

radio-qos-policy

Negates a command or resets configured settings to their default. When used in the radio QOS policy mode, the `no` command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [accelerated-multicast|admission-control|smart-aggregation|wmm|service]

no accelerated-multicast [client-timeout|max-client-streams|max-streams|
overflow-policy|stream-threshold]

no admission-control [firewall-detected-traffic|implicit-tspec|background|
best-effort|video|voice]
no admission-control [firewall-detected-traffic|implicit-tspec]
no admission-control [background|best-effort|video|voice] {max-airtime-percent|
max-clients|max-roamed-clients|reserved-for-roam-percent}

no smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}
no smart-aggregation {delay [background|best-effort|streaming-video|
video-conferencing|voice]|max-mesh-hops|min-aggregation-limit}

no wmm [background|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]

no service admission-control across-reassoc
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or resets configured settings to their default. When used in the radio QOS policy mode, the `no` command enables the resetting of accelerated multicast parameters, admission control parameters, and MultiMedia parameters.

Example

The following example shows the Radio-qos-policy 'test' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 admission-control best-effort max-clients 200
 accelerated-multicast stream-threshold 15
 accelerated-multicast client-timeout 500
rfs6000-37FABE(config-radio-qos-test)#

rfs6000-37FABE(config-radio-qos-test)#no admission-control best-effort max-
clients
rfs6000-37FABE(config-radio-qos-test)#no accelerated-multicast client-timeout
```

The following example shows the Radio-qos-policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 accelerated-multicast stream-threshold 15
rfs6000-37FABE(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
 service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#no service admission-control across-reassoc

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
rfs4000-229D58(config-radio-qos-test)#
```

17.1.4 smart-aggregation

radio-qos-policy

Configures smart aggregation parameters on this Radio QoS policy. Smart aggregation is disabled by default.

Smart aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame's typical aggregation, an aggregated frame is sent when:

- A pre-configured number of aggregated frames is reached
- An administrator-defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- An administrator-defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic might not be aggregated, but sent immediately. Whereas, background data traffic is set a delay for aggregating frames, and these aggregated frames are sent.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
smart-aggregation {delay|max-mesh-hops|min-aggregation-limit}

smart-aggregation {delay [background|best-effort|streaming-video|video-conferencing|voice] <0-1000>}

smart-aggregation {max-mesh-hops <1-10>}

smart-aggregation {min-aggregation-limit <0-64>}
```

Parameters

```
• smart-aggregation {delay [background|best-effort|streaming-video|video-conferencing|voice] <0-1000>}
```

delay	Optional. Configures the maximum delay parameter for each traffic type This is the maximum delay, in milliseconds, in the transmission of the first frame received.
background	Configures the maximum delay parameter, in milliseconds, for background traffic (250 msec)
best-effort	Configures the maximum delay parameter, in milliseconds, for best effort traffic (150 msec)
streaming-video	Configures the maximum delay parameter, in milliseconds, for streaming video traffic (150 msec)
video-conferencing	Configures the maximum delay parameter, in milliseconds, for video conference traffic (40 msec)

voice	Configures the maximum delay parameter, in milliseconds, for voice traffic (0 msec)
<0-1000>	This parameter is common to all of the above traffic types. • <0-1000> – Specify a value from 0 - 1000 msec.

- `smart-aggregation` *`{max-mesh-hops <1-10>}`*

max-mesh-hops <1-10>	Optional. Sets the maximum number of expected hops to the destination within a mesh • <1-10> – Specify a value from 1 - 10. The default is 3 hops.

- `smart-aggregation` *`{min-aggregation-limit <0-64>}`*

min-aggregation-limit <0-64>	Optional. Sets the minimum number of aggregates buffered before an aggregate is sent • <0-64> – Specify a value from 0 - 64. The default is 8 frames.

Example

```
rfs6000-37FABE(config-radio-qos-test)#smart-aggregation delay voice 50

rfs6000-37FABE(config-radio-qos-test)#smart-aggregation delay background 100

rfs6000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 smart-aggregation delay voice 50
 smart-aggregation delay background 100
rfs6000-37FABE(config-radio-qos-test)#
```

Related Commands

no	Resets the minimum aggregation limit

17.1.5 service

radio-qos-policy

Invokes service commands in the radio QoS configuration mode

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
service [admission-control|show]

service admission-control across-reassoc

service show cli
```

Parameters

- `service admission-control across-reassoc`

service	Invokes service commands
admission-control across-reassoc	Retains previously negotiated TSPEC parameters across re-associations on the radio For more information on admission-control parameters, see *admission-control*.

- `service show cli`

service show cli	Displays running system information • cli – Displays the Radio QoS mode's CLI tree

Example

```
rfs4000-229D58(config-radio-qos-test)#service admission-control across-reassoc

rfs4000-229D58(config-radio-qos-test)#show context
radio-qos-policy test
 service admission-control across-reassoc
rfs4000-229D58(config-radio-qos-test)#

rfs4000-229D58(config-radio-qos-test)#service show cli
Radio QoS Mode mode:
+-help [help]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-detailed [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-only-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show|skip-no)]
      +-skip-no [help search WORD (|detailed|only-show|skip-show|skip-no)]
+-show
  +-commands [show commands]
  +-adoption
    +-log

--More--]
```

Related Commands

no	Disables retention of previously negotiated TSPEC parameters across re-associations on the radio

17.1.6 wmm

radio-qos-policy

Configures 802.11e *wireless multimedia* (wmm) parameters

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
wmm [background|best-effort|video|voice]

wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```

Parameters

```
• wmm [background|best-effort|video|voice] [aifsn <1-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```

wmm background	Configures background access category wireless multimedia settings
wmm best-effort	Configures best effort access category wireless multimedia settings
wmm video	Configures video access category wireless multimedia settings
wmm voice	Configures voice access category wireless multimedia settings
aifsn <1-15>	Configures *Arbitrary Inter-Frame Space Number* (AIFSN) as the wait time between data frames derived from the AIFSN and slot time • background – Sets the current AIFSN for low (background) traffic. The default is 7. • best-effort – Sets the current AIFSN for normal (best-effort) traffic. The default is 3. • video – Set the current AIFSN for video traffic. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1. • voice – Sets the current AIFSN for voice traffic. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This causes lower-priority traffic to wait longer before attempting access. The default is 1. The following keyword is common to all of the above traffic types: • <1-15> – Sets a value from 1 - 15
cw-max <0-15>	Clients pick a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window. • background – Sets CW Max for low (background) traffic. The default is 10. • best-effort – Sets CW Max for normal (best effort) traffic. The default is 6. Contd..

	• voice – Sets CW Max for voice traffic. The default is 3. • video – Sets CW Max for video traffic. The default is 4 The following keyword is common to all of the above traffic types: • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). **Note:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).
cw-min <0-15>	Clients select a number between 0 and the min contention window to wait before retransmission. Clients then double their wait time on a collision, until it reaches the maximum contention window. • background – Sets CW Min for low (background) traffic. The default is 4. • best-effort – Sets CW Min for normal (best effort) traffic. The default is 4. • voice – Sets CW Min for voice traffic. The default is 2. • video – Sets CW Min for video traffic. The default is 3. The following keyword is common to all of the above traffic types: • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). **Note:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).
txop-limit <0-65535>	Set the interval, in microseconds, during which a particular client has the right to initiate transmissions • background – Sets TXOP for low (background) traffic. The default is 0. • best-effort – Sets TXOP for normal (best effort) traffic. The default is 4. • voice – Sets TXOP for voice traffic. The default is 47. • video – Sets TXOP for video traffic. The default is 94. The following keyword is common to all of the above traffic types: • <0-65535> – Specify a value from 0 - 65535 to configure the transmit opportunity limit in 32 microsecond units. **Note:** Lower values are used for higher priority traffic (like video and voice) and higher values are used for lower priority traffic (like background and best-effort).

Usage Guidelines

Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- To support QoS, each multimedia application, wireless client, and WLAN is required to support WMM.
- WMM enabled clients can co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a Best Effort access category.
- Default WMM values are recommended for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.
- Overloading an access point radio with too much high priority traffic (especially voice) degrades overall service quality for all users.
- TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TSPEC or even support WMM traffic prioritization.

Example

```
rfs6000-37FABE(config-radio-qos-test)#wmm best-effort aifsn 7
rfs6000-37FABE(config-radio-qos-test)#wmm voice txop-limit 1

rfs6000-37FABE(config-radio-qos-test)#show context
radio-qos-policy test
 wmm best-effort aifsn 7
 wmm voice txop-limit 1
 admission-control voice max-airtime-percent 9
 admission-control voice reserved-for-roam-percent 8
 accelerated-multicast stream-threshold 15
rfs6000-37FABE(config-radio-qos-test)#
```

Related Commands

no	Reverts or resets 802.11e/wireless multimedia settings to their default

18 ROLE-POLICY

This chapter summarizes the role policy commands in the CLI command structure.

A well defined role policy simplifies user management, and is a significant aspect of WLAN management. It acts as a role based firewall (much like ACLs) consisting of user-defined roles. Each role has a set of match criteria (filters) used to filter wireless clients. The action taken when a client matches the defined filters, is determined by the IP or MAC ACL associated with the user-defined role. Based on the conditions specified in the IP and/or MAC ACL, clients are granted or denied access to the controller managed network. The role policy also defines the VLAN and data rates assigned to clients provided network access.

A role policy also enables LDAP service, allowing controllers and access points to retrieve user information from the LDAP server. This information is matched with the user-defined role filters to determine if a client matches the role or not, and should be allowed or denied access to the controller managed network.

Use the (config-role-policy) instance to configure role policy related configuration commands. To navigate to the
config-role instance, use the following commands:

```
<DEVICE>(config)#role-policy <POLICY-NAME>

rfs6000-37FABE(config)#role-policy test
rfs6000-37FABE(config-role-policy-test)#?
Role Policy Mode commands:
  default-role      Configuration for Wireless Clients not matching any role
  ldap-deadperiod   Ldap dead period interval
  ldap-query        Set the ldap query mode
  ldap-server       Add a ldap server
  ldap-timeout      Ldap query timeout interval
  no                Negate a command or set its defaults
  user-role         Create a role

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
  revert            Revert changes
  service           Service Commands
  show              Show running system information
  write             Write running configuration to memory or terminal
rfs6000-37FABE(config-role-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

18.1 role-policy

- *ROLE-POLICY*

The following table summarizes role policy configuration commands:

Table 18.1 *Role-Policy-Config Commands*

Command	Description	Reference
default-role	Assigns the default role to clients not matching any of the user-defined roles defined in the role policy	*page 18-3*
ldap-deadperiod	Configures the *Lightweight Directory Access Protocol* (LDAP) deadperiod interval	*page 18-5*
ldap-query	Enables LDAP service and specifies the LDAP server query mode	*page 18-6*
ldap-server	Configures the LDAP server settings	*page 18-7*
ldap-timeout	Configures the LDAP query timeout interval	*page 18-9*
no	Negates a command or reverts settings to their default	*page 18-10*
user-role	Creates a role and associates it to the newly created role policy	*page 18-11*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

18.1.1 default-role

role-policy

Assigns a default role to a wireless client that fails to match any of the user-defined roles

When a wireless client accesses a network, the client's details, retrieved from the LDAP server, are matched against all user-defined roles within the role policy. If the client fails to match any of these user-defined role filters, the client is assigned the default role. The action taken (permit or deny access) is determined by the IP and/or MAC ACL associated with the default role.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
default-role use [ip-access-list|ipv6-access-list|mac-access-list]

default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>
```

Parameters

```
• default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
<IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>
```

default-role use	Enables default role configuration. This role is applied to a wireless client not matching any of the user-defined roles. • Use – Associates an IP, IPv6, or MAC access list with the default role
[ip-access-list| ipv6-access-list| mac-access-list] [in|out] <IP/IPv6/MAC-ACCESS-LIST-NAME>	Associates an IP access list, IPv6 access list, or a MAC access list with this default role • in – Applies the rule (IP, IPv6, or MAC) to incoming packets • out – Applies the rule (IP, IPv6, or MAC) to outgoing packets IP and MAC *access control lists* (ACLs) act as firewalls by blocking and/or permitting data traffic in both directions (inbound and outbound) within a managed network. IP ACLs use IP addresses for matching operations. Whereas, MAC ACLs use MAC addresses for matching operations, In case of a match (i.e. if a packet is received from or is destined for a specified IP or MAC address), an action is taken. This action is a typical allow, deny or mark designation to controller packet traffic. For more information on ACLs, see *AAA-POLICY*. • <IP/IPv6/MAC-ACCESS-LIST-NAME> – Specify the access list name. The ACL applied determines the action applied to a client assigned the default role.
precedence <1-100>	The following keyword is common to the all of the above parameters: • precedence – Assigns a precedence value to the ACL identified in the previous step. • <1-100> – Specify a precedence from 1 - 100. ACLs are applied in increasing order of their precedence. Rules with lower precedence are given priority.

Example

```
rfs6000-37FABE(config-role-policy-test)#default-role use ip-access-list in test
precedence 1

rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
rfs6000-37FABE(config-role-policy-test)#
```

Related Commands

no	Removes or resets the default role configuration

18.1.2 ldap-deadperiod

role-policy

Configures the LDAP deadperiod interval

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-deadperiod <60-300>
```

Parameters

- `ldap-deadperiod <60-300>`

ldap-deadperiod <60-300>	Configures a LDAP dead period. When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details to match with user-defined role filters. The LDAP deadperiod is the interval between two consecutive attempts to bind with the LDAP server. To enable LDAP service, use the *ldap-query* command. • <60-300> – Specify the interval from 60 - 300 seconds. The default is 120 seconds.

Example

```
rfs6000-37FABE(config-role-policy-test)#ldap-deadperiod 100

rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-deadperiod 100
rfs6000-37FABE(config-role-policy-test)#
```

Related Commands

no	Removes or resets the LDAP deadperiod interval

18.1.3 ldap-query

role-policy

Enables LDAP service and specifies the LDAP server query mode

Configuring the LDAP server query mode automatically enables LDAP service on this role policy. By default LDAP service is disabled.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-query [self|through-controller]
```

Parameters

- `ldap-query [self|through-controller]`

self	Configures LDAP query mode as self. The AP directly queries the LDAP server for user information. Select 'self' to use local LDAP server resources configured using the *ldap-server* command.
through-controller	Configures LDAP query mode as through-controller. The AP queries the LDAP server, for user information, through the controller. Use this option when the AP is layer 2 adopted to the controller.

Example

```
rfs6000-37FABE(config-role-policy-test)#ldap-query self

rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-deadperiod 100
rfs6000-37FABE(config-role-policy-test)#
```

Related Commands

no	Disables LDAP service on this role policy

18.1.4 ldap-server

role-policy

Associates a specified LDAP server with this role policy. Use this command to configure the credentials needed to bind with the LDAP server.

When enabled, LDAP service allows the AP or controller to bind with the LDAP server and retrieve user details. This information is matched with the user-defined roles within the role policy. If a match is made, the user is assigned the role and allowed or denied access to the controller managed network.

You can associate two LDAP servers with a role policy, allowing failover in case the primary server is unreachable.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-server <1-2> host [<IP>|<FQDN>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>} {(server-type [active-directory|
openldap])}
```

Parameters

```
• ldap-server <1-2> host [<IP>|<HOSTNAME>] bind-dn <BIND-DN> base-dn <BASE-DN>
bind-password <PASSWORD> {port <1-65535>} {(server-type [active-directory|
openldap])}
```

ldap-server <1-2>	Specify the LDAP server ID from 1 - 2. The primary LDAP server (ID 1) is used to bind and query. The secondary LDAP server (ID 2) is for failover.
host [<IP>|<FQDN>]	Specify the LDAP server's IP address or *Fully Qualified Domain Name* (FQDN).
bind-dn <BIND-DN>	Specify the bind distinguished name (used for binding with the server).
base-dn <BASE-DN>	Specify the base distinguished name (used for searching). This should not exceed 127 characters.
bind-password <PASSWORD>	Specify the LDAP server password associated with the bind DN.
port <1-65535>	Optional. Specify the LDAP server port from 1 - 65535. (default is 389).
server-type [active-directory| openldap]	The following keywords are common to the 'port' parameter: • server-type – Optional. Specifies the LDAP server type • active-directory – Enables support for active directory attribute search. This is the default setting. • openldap – Enables support for openLDAP attribute search

Usage Guidelines

Use the ldap-query command to enable LDAP service on a role policy.

Use the show > role > ldap-stats command to view LDAP server status and state.

Example

```
rfs6000-37FABE(config-role-policy-test)#ldap-server 1 host 192.168.13.7 bind-dn
"CN=Administrator,CN=Users,DC=TechPub,DC=com" base-dn "CN=Administrator,CN=Users,
DC=TechPub,DC=com" bind-password 0 superuser port 2
rfs6000-37FABE(config-role-policy-test)#

rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn
CN=Administrator,CN=Users,DC=TechPub,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
rfs6000-37FABE(config-role-policy-test)#
```

Related Commands

no	Removes or resets the LDAP server settings

18.1.5 ldap-timeout

role-policy

Configures the LDAP timeout interval. This is the interval after which a LDAP query is timed out.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ldap-timeout <1-5>
```

Parameters

- `ldap-timeout <1-5>`

ldap-timeout <1-5>	Configures the LDAP query timeout interval from 1 - 5 seconds (default is 2 seconds) When enabled, LDAP service allows the AP or controller to bind with the LDAP server and query it for user details. The LDAP query timeout is the interval between a request to and the response from the LDAP server. Once this interval is exceeded, the LDAP bind and query is timed out.

Example

```
rfs6000-37FABE(config-role-policy-test)#ldap-timeout 1

rfs6000-37FABE(config-role-policy-test)#show context
role-policy test default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn
CN=Adminstrator,CN=Users,DC=TechPub,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2
rfs6000-37FABE(config-role-policy-test)#
```

Related Commands

no	Removes or resets the LDAP query timeout to default (2 seconds)

18.1.6 no

role-policy

Negates a command or resets settings to their default. When used in the config role policy mode, the *no* command removes or resets the role policy settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [default-role|ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout|user-role]

no [ldap-deadperiod|ldap-query|ldap-server <1-2>|ldap-timeout]

no default-role use [ip-access-list|ipv6-access-list|mac-access-list]
no default-role use [ip-access-list|ipv6-access-list|mac-access-list] [in|out] <IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>

no user-role <ROLE-NAME>
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates a command or resets settings to their default. When used in the config role policy mode, the *no* command removes or resets the role policy settings.

Example

The following example shows the role policy 'test' setting before the 'no' commands are executed:

```
rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
 ldap-timeout 1
 ldap-deadperiod 100
 ldap-server 1 host 192.168.13.7 bind-dn
CN=Adminstrator,CN=Users,DC=TechPub,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 superuser port 2

rfs6000-37FABE(config-role-policy-test)#

rfs6000-37FABE(config-role-policy-test)#no ldap-deadperiod
rfs6000-37FABE(config-role-policy-test)#no ldap-timeout
rfs6000-37FABE(config-role-policy-test)#no ldap-server 1
```

The following example shows the role policy 'test' setting after the 'no' commands are executed:

```
rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 default-role use ip-access-list in test precedence 1
 ldap-query self
rfs6000-37FABE(config-role-policy-test)#
```

18.1.7 user-role

role-policy

This command creates a user-defined role. Each user-defined role has a set of Active Directory attributes. Each attribute is matched against the information returned by the LDAP server, until a complete match of role is found.

The following table summarizes user role configuration commands:

Table 18.2 *User-Role-Config Commands*

user-role	Creates a new user role and enters its configuration mode	*page 18-12*
user-role commands	Summarizes user role configuration mode commands	*page 18-14*

18.1.7.1 user-role

user-role

Creates a user-defined role. Each role consists of a set of filters and action. The filters are match criteria used to filter wireless clients. And the action defines the action taken when a client matches the specified filters.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
user-role <ROLE-NAME> precedence <1-10000>
```

Parameters

- `user-role <ROLE-NAME> precedence <1-10000>`

user-role <ROLE-NAME>	Configures the user role name • <ROLE-NAME> – Specify a name for this user role.
precedence <1-10000>	Sets the precedence for this role Lower the precedence, higher is the role priority. Precedence determines the order in which a role is applied. If a wireless client matches multiple roles, the role with the lower precedence is applied before those with higher precedence. While there is no default precedence for a role, two or more roles can share the same precedence.

Example

```
rfs6000-37FABE(config-role-policy-test)#user-role testing precedence 10
rfs6000-37FABE(config-role-policy-test)#show context
role-policy test
 user-role testing precedence 10
 default-role use ip-access-list in test precedence 1
rfs6000-37FABE(config-role-policy-test)#

rfs6000-37FABE(config-role-policy-test-user-role-testing)#?
Role Mode commands:
  ap-location           AP Location configuration
  assign                Assign parameters to the role
  authentication-type   Type of Authentication
  captive-portal        Captive-portal based Role Filter
  city                  City configuration
  client-identity       Client identity
  company               Company configuration
  country               Country configuration
  department            Department configuration
  emailid               Emailid configuration
  employee-type         Employee-type configuration
  employeeid            Employeeid configuration
  encryption-type       Type of encryption
  group                 Group configuration
  memberOf              MemberOf configuration
  mu-mac                MU MAC address configuration
  no                    Negate a command or set its defaults
  radius-user           Radius-user configuration
  ssid                  SSID configuration
```

```
  state                 State configuration
  title                 Title configuration
  use                   Set setting to use
  user-defined          User-defined configuration

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes an existing user role

18.1.7.2 user-role commands

user-role

The following table summarizes user role configuration mode commands:

Table 18.3 *User-Role-Mode Commands*

Commands	Description	Reference
ap-location	Configures an AP deployment location based filter	*page 18-15*
assign	Configures upstream/downstream rate limits and VLAN ID assigned to clients matching the filters defined in the user-defined role	*page 18-16*
authentication-type	Configures an authentication type based filter	*page 18-18*
captive-portal	Configures a captive portal based filter	*page 18-20*
city	Configures a city name based filter	*page 18-21*
client-identity	Associates a client-identity (device fingerprinting) based filter	*page 18-22*
company	Configures a company name based filter	*page 18-23*
country	Configures a country name based filter	*page 18-25*
department	Configures a department name based filter	*page 18-27*
emailid	Configures a e-mail ID based filter	*page 18-29*
employee-type	Configures a employee type ID based filter	*page 18-31*
employeeid	Configures a employee ID based filter	*page 18-32*
encryption-type	Configures an encryption type filter	*page 18-34*
group	Configures a RADIUS group based filter	*page 18-36*
memberOf	Assigns an *Active Directory* (AD) group to this user-defined role	*page 18-38*
mu-mac	Configures MAC address and mask based filter	*page 18-39*
no	Removes or resets the filters configured on this user-defined role	*page 18-40*
radius-user	Configures a wireless client filter based on the RADIUS user name	*page 18-42*
ssid	Configures a SSID based filter	*page 18-44*
state	Configures a user role state to match	*page 18-46*
title	Configures a 'title' string to match	*page 18-48*
use	Associates a IP and/or MAC ACL with this role. These ACLs specify the action taken when a client matches this user-defined role.	*page 18-49*
user-defined	Defines a filter based on an attribute defined in the Active Directory or the OpenLDAP server	*page 18-52*

18.1.7.2.1 ap-location

user-role commands

Configures an AP's deployment location based filter for this user-defined role

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ap-location [any|contains|exact|not-contains]

ap-location any

ap-location [contains|exact|not-contains] <WORD>
```

Parameters

- `ap-location any`

ap-location any	Specifies the AP location to match (in a RF Domain) or the AP's resident configuration • any – Defines an AP's location as any

- `ap-location [contains|exact|not-contains] <WORD>`

ap-location	Specifies the AP location to match (in a RF Domain) or the AP's resident configuration. Select one of the following filter options: contains, exact, or not-contains.
contains <WORD>	Applies role if the associating AP's location contains the location string specified in the role. • <WORD> – Specify the location string to match.
exact <WORD>	Applies role if the associating AP's location exactly matches the string specified in the role. • <WORD> – Specify the exact location string to match.
not-contains <WORD>	Applies role if the associating AP's location does not contain the location string specified in the role. • <WORD> – Specify the location string not to match.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#ap-location contains
office

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ap-location contains office
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes an AP's deployment location string from this user-defined role

18.1.7.2.2 assign

user-role commands

Configures upstream/downstream rate limits and VLAN ID. Clients matching this user-defined role filters are associated with the specified VLAN, and assigned the specified data rates.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
assign [rate-limit|VLAN]

assign rate-limit [from-client|to-client] <1-65536>
assign vlan <1-4094>
```

Parameters

- `assign rate-limit [from-client|to-client] <1-65536>`

assign rate-limit [from-client|to-client] <1-65536>	Assigns an upstream and downstream traffic rate limit • from-client – Assigns a rate limit, in Kbps, for the upstream (from client) traffic • to-client – Assigns a rate limit, in Kbps, for the downstream (to client) traffic • <1-65536> – Specify upstream and/or downstream rate limits from 1 - 65536 Kbps. Wireless clients matching this user-defined role are assigned the configured rate limits.

- `assign vlan <1-4094>`

assign vlan <1-4094>	Assigns a VLAN (identified by VLAN's ID). Clients matching this user-defined role are associated with the specified VLAN. The VLAN ID represents the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). This feature is disabled by default. • <1-4094> – Specify the VLAN ID from 1 - 4094. A wireless client that fails to match any user-defined role is assigned to the default role (configured as a role policy setting) and is mapped to the default VLAN under the WLAN.

Usage Guidelines

ACLs can only be used with tunnel or isolated-tunnel modes. They do not work with the local and automatic modes.

In case of bridge VLAN, the default bridging mode is 'auto'. Change the bridging mode to 'tunnel'. This extends the controller's existing VLAN onto the AP and ensures that wireless clients are served IP addresses.

The VLAN configured under the user-defined role need not exist under the WLAN. But, when using tunneled VLAN bridges, configure an additional bridge VLAN. If the VLAN bridging mode is 'local', no additional VLAN configuration is required.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test)#assign rate-limit to-
client 200

rfs4000-229D58(config-role-policy-test-user-role-test)#commit

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
  assign vlan 1
  assign rate-limit to-client 200
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

The following examples define a role used to forward the IP traffic from all engineers in Test_Company, Santa Clara, USA onto VLAN 2.

1 Create a new role policy with name 'test-policy'.

```
<DEVICE>(config)#role-policy test-policy
```

2 Specify the LDAP server used for this role policy.

```
<DEVICE>(config-role-policy-test-policy)#ldap-query self
<DEVICE>(config-role-policy-test-policy)#ldap-server 1 host 192.160.1.1 bind-dn
CN=Administrator,CN=Users,DC=testtest,DC=com base-dn
CN=Administrator,CN=Users,DC=com bind-password 0 test port 389
<DEVICE>(config-role-policy-test-policy)#ldap-timeout 2
```

3 Create a user defined role.

```
<DEVICE>(config-role-policy-test-policy)#user-role SCEngineer precedence 100
```

4 Define the role by adding appropriate values and match operators.

```
<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#city exact santa-
clara
<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#company exact
ExampleCompany
<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#country exact usa
<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#title contains
engineer
<DEVICE>(config-role-policy-test-policy-user-role-SCEngineer)#assign vlan-id 2
```

5 Apply role policy to an access point.

```
ap7131-99BFA8(config-device-ap7131)# use role-policy test-policy
```

Related Commands

no	Removes the upstream and/or downstream rate limits applied to this user-defined role. Also removes the VLAN ID.

18.1.7.2.3 authentication-type

user-role commands

Configures the authentication type based filter for this user-defined role

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
authentication-type [any|eq|neq]
authentication-type any
authentication-type [eq|neq] [eap|kerberos|mac-auth|none]
   {(eap|kerberos|mac-auth|none)}
```

Parameters

- `authentication-type any`

any	The authentication type is any (eq or neq). This is the default setting.

- `authentication-type [eq|neq] [eap|kerberos|mac-auth|none] {(eap|kerberos|mac-auth|none)}`

eq [eap|kerberos| mac-auth|none]	The role is applied only when the authentication type matches (equals) one or more than one of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used These parameters are recursive, and you can configure more than one unique authentication type for this user-defined role.
neq [eap|kerberos| mac-auth|none]	The role is applied only when the authentication type does not match (not equals) any of the following types: • eap – Extensible authentication protocol • kerberos – Kerberos authentication • mac-auth – MAC authentication protocol • none – no authentication used These parameters are recursive, and you can configure more than one unique 'not equal to' authentication type for this user-defined role.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#authentication-type eq
kerberos

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the authentication type filter configured for this user-defined role

18.1.7.2.4 captive-portal

user-role commands

Configures a captive portal based filter for this user-defined role. A captive portal is a guest access policy that provides temporary and restrictive access to the wireless network. When applied to a WLAN, a captive portal policy ensures secure guest access.

This command defines user-defined role filters based on a wireless client's state of authentication.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
captive-portal authentication-state [any|post-login|pre-login]
```

Parameters

- `captive-portal authentication-state [any|post-login|pre-login]`

authentication-state	Defines the authentication state of a client connecting to a captive portal
any	Specifies any authentication state (authenticated and pending authentication). This is the default setting. This option makes no distinction on whether authentication is conducted before or after the wireless client has logged in.
post-login	Specifies authentication is completed successfully This option requires the wireless client to share authentication credentials after logging into the managed network.
pre-login	Specifies authentication is pending This option enables captive portal client authentication before the client is logged into the controller.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#captive-portal
authentication-state pre-login

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the captive portal based role filter settings

18.1.7.2.5 city

user-role commands

Configures a wireless client filter based on the city name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
city [any|contains|exact|not-contains]
city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `city [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

city	Specifies a wireless client filter based on how the 'city' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contain.
any	No specific city associated with this user-defined role. This role can be applied to any wireless client from any city.
contains <WORD>	The role is applied only when the city name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the city name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the city name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the city name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#city exact SanJose

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the city name configured with this user-defined role

18.1.7.2.6 client-identity

user-role commands

Associates a client-identity (device fingerprinting) based filter. The role is assigned to a wireless client matching any of the defined client identities.

For more information on configuring client identity fingerprints, see *client-identity*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}
```

Parameters

- `client-identity <CLIENT-IDENTITY-NAME> {<CLIENT-IDENTITY-NAME>}`

client-identity <CLIENT-IDENTITY-NAME>	Specifies the client-identity fingerprint to match (should be existing and configured) • <CLIENT-IDENTITY-NAME> – Specify the client identity signature name. Multiple client identities can be configured with a role policy.

Usage Guidelines

When associating a single or multiple client identities with a role policy, ensure that in a client identity group, all the client identities used by the role policy, is attached to the device or profile using the role policy. In other words, group all the client identities (used in this role policy) in a client identity group, and associate this group to the profile or device using this role policy.

For more information on configuring client identities and client identity groups, see *client-identity* and *client-identity-group*.

For more information on associating a client identity group and a role policy to a profile or a device, see *use*.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test)#client-identity
TestClientIdentity
rfs4000-229D58(config-role-policy-test-user-role-test)#commit

rfs4000-229D58(config-role-policy-test-user-role-test)#client-identity
ClientIdentityWindows
rfs4000-229D58(config-role-policy-test-user-role-test)#

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
  client-identity TestClientIdentity
  client-identity ClientIdentityWindows
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

Related Commands

no	Removes the client identities associated with this role policy

18.1.7.2.7 company

user-role commands

Configures a wireless client filter based on the company name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
company [any|contains|exact|not-contains]
company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `company [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

company	Specifies a wireless client filter based on how the 'company' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific company associated with this user-defined role. This role is applied to any wireless client from any company (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the company name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the company name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the company name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the company name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#company exact
ExampleCompany

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the company name configured with this user-defined role

18.1.7.2.8 country

user-role commands

Configures a wireless client filter based on the country name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
country [any|contains|exact|not-contains]
country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `country [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

country	Specifies a wireless client filter based on how the 'country' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific country associated with this user-defined role. This role is applied to any wireless client from any country (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the country name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the country name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the country name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the country name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#country exact America

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact Examplecompany
  country exact America
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the country name configured with this user-defined role

18.1.7.2.9 department

user-role commands

Configures a wireless client filter based on the department name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
department [any|contains|exact|not-contains]
department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `department [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

department	Specifies a wireless client filter based on how the 'department' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific department associated with this user-defined role. This role can be applied to any wireless client from any department (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the department name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the department name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the department name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the department name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#department exact TnV

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the department name configured with this user-defined role

18.1.7.2.10 emailid

user-role commands

Configures a wireless client filter based on the e-mail ID

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
emailid [any|contains|exact|not-contains]
emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `emailid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

emailid	Specifies a wireless client filter based on how the 'e-mail ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	No specific e-mail ID associated with this user-defined role. This role can be applied to any wireless client having any e-mail ID (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the e-mail ID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the e-mail ID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the e-mail ID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the e-mail ID returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#emailid exact testing@
examplecompany.com

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the e-mail ID configured with this user-defined role

18.1.7.2.11 employee-type

user-role commands

Configures a wireless client filter based on the employee type

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
employee-type [any|contains|exact|not-contains]
employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `employee-type [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

employee-type	Specifies a wireless client filter based on how the 'employee type', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	No specific employee type associated with this user-defined role. This role can be applied to any wireless client having any employee type (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the employee type, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the employee type, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the employee type, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the employee type returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test1)#employee-type exact
consultant

rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
 user-role user1 precedence 1
  employee-type exact consultant
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

Related Commands

no	Removes the employee type filter configured with this user-defined role

18.1.7.2.12 employeeid

user-role commands

Configures a wireless client filter based on the employee ID

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
employeeid [any|contains|exact|not-contains]
employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]
```

Parameters

- `employeeid [any|exact <WORD>|contains <WORD>|not-contains <WORD>]`

employeeid	Specifies a wireless client filter based on how the 'employee ID', returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	No specific employee ID associated with this user-defined role. This role can be applied to any wireless client having any employee ID (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the employee ID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should contain the provided expression.
exact	The role is applied only when the employee ID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the employee ID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the employee ID returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#employeeid contains
TnVTest1

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnVTest1
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the employee ID configured with this user-defined role

18.1.7.2.13 encryption-type

user-role commands

Selects the encryption type for this user-defined role. Encryption ensures privacy between access points and wireless clients. There are various modes of encrypting communication on a WLAN, such as *Counter-model CBC-MAC Protocol* (CCMP), *Wired Equivalent Privacy* (WEP), keyguard, *Temporal Key Integrity Protocol* (TKIP), etc.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
encryption-type [any|eq|neq]

encryption-type any

encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64]
(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)}
```

Parameters

- `encryption-type any`

any	The encryption type can be any one of the listed options (ccmp|keyguard|tkip|wep128|wep64). This is the default setting.

- `encryption-type [eq|neq] [ccmp|keyguard|none|tkip|wep128|wep64] {(ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep64)}`

eq [ccmp|keyguard|none|tkip|wep128|wep64]	The role is applied only if the encryption type equals to one of the following options: • ccmp – Encryption mode is CCMP • keyguard – Encryption mode is keyguard. Keyguard encryption shields the master encryption keys from being discovered. • none – No encryption mode specified • tkip – Encryption mode is TKIP • wep128 – Encryption mode is WEP128 • wep64 – Encryption mode is WEP64 These parameters are recursive, and you can configure more than one encryption type for this user-defined role.
neq [ccmp|keyguard|none|tkip|wep128|wep64]	The role is applied only if encryption type is not equal to any of the following options: • ccmp – Encryption mode is not equal to CCMP • keyguard – Encryption mode is not equal to keyguard • none: Encryption mode is not equal to none • tkip – Encryption mode is not equal to TKIP Contd..

	• wep128 – Encryption mode is not equal to WEP128 • wep64 – Encryption mode is not equal to WEP64 These parameters are recursive, and you can configure more than one 'not equal to' encryption type for this user-defined role.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#encryption-type eq
wep128

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnVTest1
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the encryption type configured for this user-defined role

18.1.7.2.14 group

user-role commands

Configures a wireless client filter based on the RADIUS group name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
group [any|contains|exact|not-contains]
group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

- `group [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

group	Specifies a wireless client filter based on how the RADIUS group name matches the provided expression. Select one of the following options: any, contains, exact, or not-contains
any	This user-defined role can fit into any group (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the RADIUS group name contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the RADIUS group name exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the RADIUS group name does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the group name returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#group contains
testgroup

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact Example_company
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnVTest1
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the group configured for this user-defined role

18.1.7.2.15 memberOf

user-role commands

Applies an *Active Directory* (AD) group filter to this user-defined role. A wireless client can be a member of more than one group within the AD database. This command applies a AD group based firewall, which applies a role to a wireless client only if it belongs to the specified AD group.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
memberOf <AD-GROUP-NAME>
```

Parameters

- `memberOf <AD-GROUP-NAME>`

memberOf <AD-GROUP-NAME>	Applies this user-defined role to a client only if the client belongs to the specified AD group • <AD-GROUP-NAME> – Specify the AD group name.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-test)#memberOf ADTestgroup

rfs4000-229D58(config-role-policy-test-user-role-test)#show context
 user-role test precedence 1
  assign vlan 1
  assign rate-limit to-client 200
  memberOf ADTestgroup
rfs4000-229D58(config-role-policy-test-user-role-test)#
```

Related Commands

no	Removes the AD group assigned to this user-defined role

18.1.7.2.16 mu-mac

user-role commands

Configures a MAC address and mask based filter for this role policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mu-mac [<MAC>|any]

mu-mac any

mu-mac <MAC> {mask <MAC>}
```

Parameters

- `mu-mac any`

any	Applies role to any wireless client (no MAC address to match). This is the default setting.

- `mu-mac <MAC> {mask <MAC>}`

<MAC>	Applies role to the wireless client having specified MAC address • <MAC> – Sets the MAC address in the AA-BB-CC-DD-EE-FF format
mask <MAC>	Optional. After specifying the client's MAC address, specify the mask in the AA-BB-CC-DD-EE-FF format. The role is applied to the wireless client exactly matching the specified MAC address and MAC mask.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#mu-mac 11-22-33-44-55-
66

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  mu-mac 11-22-33-44-55-66
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnVTest1
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the MAC address and mask for this user-defined role

18.1.7.2.17 no

user-role commands

Negates a command or resets configured settings to their default. When used in the config role policy user-defined role mode, the no command removes or resets settings, such as AP location, authentication type, encryption type, captive portal, etc.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [ap-location|assign|authentication-type|captive-portal|city|client-identity|
   company|country|department|emailid|employee-type|employeeid|encryption-type|
   group|memberOf|mu-mac|radius-user|ssid|state|title|use|user-defined]

no [ap-location|assign|authentication-type|city|client-identity|company|country|
   department|emailid|employee-type|employeeid|encryption-type|group|mu-
mac|memberOf|
   ssid|radius-user|state|title|user-defined]

no captive-portal authentication-state

no use [application-policy|bonjour-gw-discovery-policy|ip-access-list|
   ipv6-access-list|mac-access-list|url-filter]

no use [ip-access-list|ipv6-access-list|mac-access-list] [in|out]
   <IP/IPv6/MAC-ACCESS-LIST-NAME> precedence <1-100>

no use [application-policy|bonjour-gw-discovery-policy|url-filter]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates a command or resets configured settings to their default. When used in the config role policy user-defined role mode, the no command removes or resets settings, such as AP location, authentication type, encryption type, captive portal, etc.

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example shows the Role Policy ‘test’ User Role ‘testing’ configuration before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  authentication-type eq kerberos
  encryption-type eq wep128
  ap-location contains office
  mu-mac 11-22-33-44-55-66
  group contains testgroup
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  employeeid contains TnVTest1
rfs6000-37FABE(config-role-policy-test-user-role-testing)#

rfs6000-37FABE(config-role-policy-test-user-role-testing)#no authentication-type
rfs6000-37FABE(config-role-policy-test-user-role-testing)#no encryption-type
rfs6000-37FABE(config-role-policy-test-user-role-testing)#no group
rfs6000-37FABE(config-role-policy-test-user-role-testing)#no mu-mac
rfs6000-37FABE(config-role-policy-test-user-role-testing)#no ap-location
rfs6000-37FABE(config-role-policy-test-user-role-testing)#no employeeid
```

The following example shows the Role Policy ‘test’ User Role ‘testing’ configuration after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

18.1.7.2.18 radius-user

user-role commands

Configures a wireless client filter based on the RADIUS user name

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
radius-user [any|contains|ends-with|exact|not-contains|starts-with]
```

Parameters

- `radius-user [any|contains|ends-with|exact|not-contains|starts-with]`

radius-user	Specifies a wireless client filter based on how the 'radius-user' name, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	No specific RADIUS user name associated with this user-defined role. This role can be applied to any wireless client (no strings to match). This is the default setting.
contains <WORD>	The role is applied only when the 'radius-user' name, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should contain the provided expression. You can use the realm or any sub-string of the user name.
ends-with <WORD>	Enables role assignment on the basis of the wireless client's "department" and/or "group" • <WORD> – Specify the string (could be department/group code). For example: 1005000002. In this the last three digits represent the department/group code. The remaining digits represent user's badge number. The role is applied only when the 'radius-user' name, returned by the RADIUS server, ends with the string specified here.
exact <WORD>	The role is applied only when the 'radius-user' name, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should be an exact match. Provide the complete user name along with the realm.
not-contains <WORD>	The role is applied only when the 'radius-user' name, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the 'radius-user' name returned by the RADIUS server). It should not contain the provided expression.

starts-with <WORD>	Enables role assignment on the basis of the wireless client's "department" and/or "group" code • <WORD> – Specify the string (could be department/group code). For example: 0026100573. The first three digits represent the department/group code. The remaining digits represent user's badge number. The role is applied only when the 'radius-user' name, returned by the RADIUS server, starts with the string specified here.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#radius-user contains
test.com

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 1
  radius-user contains test.com
  company exact ExampleCompany
  emailid exact testing@examplecompany.com
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the radius-user filter

18.1.7.2.19 ssid

user-role commands

Configures a SSID based filter

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ssid [any|exact|contains|not-contains]

ssid any

ssid [exact|contains|not-contains] <WORD>
```

Parameters

- `ssid any`

ssid any	Specifies a wireless client filter based on how the SSID is specified in a WLAN • any – The role is applied to any SSID location. This is the default setting.

- `ssid [exact|contains|not-contains] <WORD>`

ssid	Specifies a wireless client filter based on how the SSID is specified in a WLAN. This options are: contains, exact, or not-contains
exact <WORD>	The role is applied only when the SSID, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.
contains <WORD>	The role is applied only when the SSID, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the SSID string to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.
not-contains <WORD>	The role is applied only when the SSID, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the SSID string not to match. The SSID is case sensitive and is compared against the SSID configured for the WLAN.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#ssid not-contains
DevUser

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
rfs6000-37FABE(config-role-policy-test-user-role-testing)#]
```

Related Commands

no	Removes the SSID configured for a user-defined role

18.1.7.2.20 state

user-role commands

Configures a user role state to match with this user-defined role

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
state [any|contains|exact|not-contains]
state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

- `state [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

state	Specifies a wireless client filter option based on how the RADIUS state matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	This user role can fit any wireless client irrespective of the state (no strings to match).
contains <WORD>	The user role is applied only when the RADIUS state contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the RADIUS state exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the RADIUS state does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the state returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#state exact active

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  state exact active
rfs6000-37FABE(config-role-policy-test-user-role-testing)#
```

Related Commands

no	Removes the ‘state’ filter string associated with a user role

18.1.7.2.21 title

user-role commands

Configures a 'title' string to match

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
title [any|contains|exact|not-contains]
title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

- `title [any|contains <WORD>|exact <WORD>|not-contains <WORD>]`

title	Specifies a wireless client filter based on how the title string, returned by the RADIUS server, matches the provided expression. Select one of the following options: any, contains, exact, or not-contains.
any	This user role can fit any wireless client irrespective of the title (no strings to match).
contains <WORD>	The user role is applied only when the title string, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the title string, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the title string, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the title returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#title any
```

Related Commands

no	Removes the 'title' filter string configured with a user role

18.1.7.2.22 use

user-role commands

Configures an access list based firewall with this user role

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, firewalls are mechanisms both *blocking* and *permitting* data traffic based on inbound and outbound IP and MAC rules.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same layer 2 interface can be filtered by applying both an IP ACL and a MAC.

A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [application-policy|bonjour-gw-discovery-policy|ip-access-list|ipv6-access-
list|mac-access-list|url-filter]

use bonjour-gw-discovery-policy <POLICY-NAME>

use [ip-access-list|ipv6-access-list] [in|out] <IP/ipv6-ACCESS-LIST-NAME>
   precedence <1-100>

use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>

use url-filter <URL-FILTER-NAME>
```

Parameters

- `use application-policy|bonjour-gw-discovery-policy] <POLICY-NAME>`

application-policy <POLICY-NAME>	Uses an existing Application policy with a user role. When associated, the Application policy enforces application assurance for all users using this role. • <POLICY-NAME> – Specify the Application policy name (should be existing and configured). For more information on Application policy, see *application-policy*.
bonjour-gw-discovery-policy <POLICY-NAME>	Uses an existing Bonjour GW Discovery policy with a user role. When associated, the Bonjour GW Discovery policy is applied for the Bonjour requests coming from this specific user roles. • <POLICY-NAME> – Specify the Bonjour GW Discovery policy name (should be existing and configured). For more information on Bonjour GW Discovery policy, see *bonjour-gw-discovery-policy*.

- `use [ip-access-list|ipv6-access-list] [in|out] <IP/IPv6-ACCESS-LIST-NAME> precedence <1-100>`

ip-access-list [in|out]	Uses an IPv4 or IPv6 ACL with this user role • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<IPv4/IPv6-ACCESS-LIST-NAME>	Specify the IPv4/IPv6 access list name.
precedence <1-100>	After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first. • <1-100> – Sets a precedence from 1 - 100

- `use mac-access-list [in|out] <MAC-ACCESS-LIST-NAME> precedence <1-100>`

mac-access-list [in|out]	Uses a MAC access list with this user role • in – Applies the rule to incoming packets • out – Applies the rule to outgoing packets
<MAC-ACCESS-LIST-NAME>	Specify the MAC access list name.
precedence <1-100>	After specifying the name of the access list, specify the precedence applied to it. Based on the packets received, a lower precedence value is evaluated first • <1-100> – Sets a precedence from 1 - 100

- `use url-filter <URL-FILTER-NAME>`

use url-filter <URL-FILTER-NAME>	Uses an existing URL filter that acts as a Web content filter firewall rule. • <POLICY-NAME> – Specify the URL filter name (should be existing and configured).

Example

```
rfs6000-37FABE(config-role-policy-test-user-role-testing)#use ip-access-list in
test precedence 9

rfs6000-37FABE(config-role-policy-test-user-role-testing)#show context
 user-role testing precedence 10
  ssid not-contains DevUser
  captive-portal authentication-state pre-login
  city exact SanJose
  company exact ExampleCompany
  country exact America
  department exact TnV
  emailid exact testing@examplecompany.com
  state exact active
  use ip-access-list in test precedence 9
rfs6000-37FABE(config-role-policy-test-user-role-testing)#

rfs6000-37FABE(config-role-policy-bonjour_test-user-role-bonjour_user1)#use
bonjour-gw
-discovery-policy role2

rfs6000-37FABE(config-role-policy-bonjour_test-user-role-bonjour_user1)#show
context
 user-role bonjour_user1 precedence 2
  use bonjour-gw-discovery-policy role2
rfs6000-37FABE(config-role-policy-bonjour_test-user-role-bonjour_user1)#
```

```
rfs6000-37FABE(config-role-policy-bonjour_test)#show context
role-policy bonjour_test
 user-role bonjour_user precedence 1
  mu-mac A4-D1-D2-BF-3D-19
  use bonjour-gw-discovery-policy role1
 user-role bonjour_user1 precedence 2
  mu-mac B0-65-BD-4B-BC-09
  use bonjour-gw-discovery-policy role2
.....................................................
rfs6000-37FABE(config-role-policy-bonjour_test)#
```

Related Commands

no	Removes an IP, MAC access list, or a Bonjour GW Discovery policy from use with a user role

18.1.7.2.23 user-defined

user-role commands

Enables you to define a filter based on an attribute defined in the Active Directory or the OpenLDAP server

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
user-defined <ATTR-STRING> [any|contains|exact|not-contains]

user-defined <ATTR-STRING> [any|contains <WORD>|exact <WORD>|not-contains <WORD>]
```

Parameters

```
• user-defined <ATTR-STRING> [any|exact <WORD>|contains <WORD>|not-contains
<WORD>]
```

user-defined <ATTR-STRING>	Specify a filter based on an attribute defined in the AD or OpenLDAP server. • <ATTR-NAME> – Specify the attribute string. After specifying the attribute name, specify the match type.
any	No specific string to match. This role can be applied to any wireless client. This is the default setting.
contains <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, contains the string specified in the role. • <WORD> – Specify the string to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should contain the provided expression.
exact <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, exactly matches the string specified in the role. • <WORD> – Specify the exact string to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should be an exact match.
not-contains <WORD>	The role is applied only when the user-defined attribute value, returned by the RADIUS server, does not contain the string specified in the role. • <WORD> – Specify the string not to match (this is case sensitive, and is compared against the value returned by the RADIUS server). It should not contain the provided expression.

Example

```
rfs4000-229D58(config-role-policy-test-user-role-user1)#user-defined office-
location exact EcoSpace

rfs4000-229D58(config-role-policy-test-user-role-user1)#show context
 user-role user1 precedence 1
  employee-type exact consultant
  user-defined office-location exact EcoSpace
rfs4000-229D58(config-role-policy-test-user-role-user1)#
```

Related Commands

no	Removes the user-defined filter configured with this user role

19 SMART-RF-POLICY

This chapter summarizes *Self Monitoring at Run Time RF* (Smart RF) management policy commands in the CLI command structure.

A Smart RF management policy defines operating and recovery parameters that can be assigned to groups of access points. A Smart RF policy is designed to scan the network to identify the best channel and transmit power for each access point radio.

A Smart RF policy reduces deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each managed radio. Smart RF policies when applied to specific RF Domains, apply site specific deployment configurations and self-healing values to groups of devices within pre-defined physical RF coverage areas.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through the periodic re-calibration of the network. Re-calibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).

Smart RF also provides self-healing functions by monitoring the network in real-time, and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual re-configuration to resolve.

Smart RF is supported on any RF Domain manager. In standalone environments, an individual wireless controller manages the calibration and monitoring phases. In clustered environments, a single wireless controller is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Keep in mind that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks channels specified in the Smart RF policy
- If no SMART RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring access point detect radar. The access point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using the *dfs-rehome* command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

NOTE: Perform RF planning to ensure overlapping coverage exists at a deployment site, for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it is a temporary measure. You need to determine the root cause of RF deterioration and fix it. Smart RF history/ events can assist in trouble shooting.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the Smart RF policy instance, use the following commands:

```
<DEVICE>(config)#smart-rf-policy <POLICY-NAME>

rfs6000-37FABE(config)#smart-rf-policy test

rfs6000-37FABE(config-smart-rf-policy-test)#?
Smart RF Mode commands:
  area                      Specify channel list/ power for an area
  assignable-power          Specify the assignable power during power-assignment
  avoidance-time            Time to avoid a channel once dfs/adaptivity
                            avoidance is necessary
  channel-list              Select channel list for smart-rf
  channel-width             Select channel width for smart-rf
  coverage-hole-recovery    Recover from coverage hole
  enable                    Enable this smart-rf policy
  group-by                  Configure grouping parameters
  interference-recovery     Recover issues due to excessive noise and
                            interference
  neighbor-recovery         Recover issues due to faulty neighbor radios
  no                        Negate a command or set its defaults
  sensitivity               Configure smart-rf sensitivity (Modifies various
                            other smart-rf configuration items)
  smart-ocs-monitoring      Smart off channel scanning

  clrscr                    Clears the display screen
  commit                    Commit all changes made in this session
  end                       End current mode and change to EXEC mode
  exit                      End current mode and down to previous mode
  help                      Description of the interactive help system
  revert                    Revert changes
  service                   Service Commands
  show                      Show running system information
  write                     Write running configuration to memory or terminal

rfs6000-37FABE(config-smart-rf-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

19.1 smart-rf-policy

SMART-RF-POLICY

The following table summarizes Smart RF policy configuration commands:

Table 19.1 *Smart-RF-Policy-Config Commands*

Command	Description	Reference
area	Configures the channel list and power for a specified area	*page 19-4*
assignable-power	Specifies the power range during power assignment	*page 19-5*
avoidance-time	Allows Smart RF-enabled radios to avoid *Dynamic Frequency Selection* (DFS) and/or *adaptivity* regulated channels on detection of interference or radar. This command configures the period for which the channel is avoided.	*page 19-5*
channel-list	Assigns the channel list for the selected frequency	*page 19-8*
channel-width	Selects the channel width for Smart RF configuration	*page 19-9*
coverage-hole-recovery	Enables recovery from errors	*page 19-11*
enable	Enables a Smart RF policy	*page 19-13*
group-by	Configures grouping parameters	*page 19-14*
interference-recovery	Recovers issues due to excessive noise and interference	*page 19-15*
neighbor-recovery	Enables recovery from errors due to faulty neighbor radios	*page 19-17*
no	Negates a command or reverts settings to their default	*page 19-19*
sensitivity	Configures Smart RF sensitivity	*page 19-21*
smart-ocs-monitoring	Applies smart off-channel scanning instead of dedicated detectors	*page 19-23*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

19.1.1 area

smart-rf-policy

Configures the channel list and power for a specified area

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
area <AREA-NAME/STRING-ALIAS> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>
```

Parameters

- `area <AREA-NAME/STRING-ALIAS> channel-list [2.4GHz|5GHz] <CHANNEL-LIST>`

area <AREA-NAME/ STRING-ALIAS>	Specifies the area name • <AREA-NAME/STRING-ALIAS> – Specify the area name as clear text. Alternately, use a string-alias to specify the area name. If using a string-alias, ensure that the string-alias is existing and configured.
channel-list [2.4GHz|5GHZ] <CHANNEL-LIST>	Selects the channels for the specified area in the 2.4 GHz or 5.0 GHz band • 2.4GHz – Selects the channels for the specified area in the 2.4 GHz band • 5GHz – Selects the channels for the specified area in the 5.0 GHz band The following keyword is common to the 2.4 GHz and 5.0 GHz bands: • <CHANNEL-LIST> – Enter a comma-separated list of channels for the selected band.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#area test channel-list 2.4GHz 1,2,3

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
rfs6000-37FABE(config-smart-rf-policy-test)#

nx9500-6C8809(config)#alias string $AREA Ecospace
nx9500-6C8809(config)#commit
nx9500-6C8809(config-smart-rf-policy-test)#exit

nx9500-6C8809(config-smart-rf-policy-Ecospace)#area $AREA channel-list 5GHz 36,44

nx9500-6C8809(config-smart-rf-policy-Ecospace)#show context
smart-rf-policy Ecospace
 area $AREA channel-list 5GHz 36,44
nx9500-6C8809(config-smart-rf-policy-Ecospace)#
```

Related Commands

no	Removes channel list/power configuration for an area

19.1.2 assignable-power

smart-rf-policy

Configures the Smart RF power settings over both 2.4 GHZ and 5.0 GHZ radios

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
assignable-power [2.4GHz|5GHz] [max|min] <1-20>
```

Parameters

- `assignable-power [2.4GHz|5GHz] [max|min] <1-20>`

2.4GHz [max|min] <1-20>	Assigns a power range on the 2.4 GHz band • max <1-20> – Sets the upper limit in the range from 1 dBm - 20 dBm (default is 17 dBm) • min <1-20> – Sets the lower limit in the range from 1 dBm - 20 dBm (default is 4 dBm)
5GHz [max|min] <1-20>	Assigns a power range on the 5.0 GHz band • max <1-20> – Sets the upper limit in the range from 1 dBm - 20 dBm (default is 17 dBm) • min <1-20> – Sets the lower limit in the range from 1 dBm - 20 dBm (default is 4 dBm)

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#assignable-power 5GHz max 20

rfs6000-37FABE(config-smart-rf-policy-test)#assignable-power 5GHz min 8

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Resets assignable power to its default

19.1.3 avoidance-time

smart-rf-policy

Allows *Smart-RF enabled* radios to avoid channels with high levels of *interference* and channels where *radar* has been detected

This command configures the interval for which a channel is avoided on detection of interference or radar, and is applicable only if the channel selection mode is set to Smart and a Smart-RF policy is applied to the access point's RF Domain. For more information on configuring a radio's channel of operation, see *channel*.

Certain 5.0 GHz channels are subject to FCC / ETSI DFS regulations that require channels transmitting critical radar signals to be free of interference from radio signals. Consequently, DFS-enabled 5.0 GHz radios scan and switch channels if radar is detected on their current channel of operation. If radar-free channels are not available, the radio stops transmitting until it identifies a radar-free channel.

Adaptivity is a new *European Union* (EU) stipulation that requires access points to monitor interference levels on their current channel of operation, and stop functioning on channels with interference levels exceeding ETSI-specified threshold values. When enabled, this feature ensures recovery by switching the radio to a new channel with less interference.

Once adaptivity or DFS is triggered, the radio's channel is switched based on the channel selection mode specified. If the channel is fixed, the radio attempts to come back to its specified channel of operation after the DFS/adaptivity channel evacuation period has expired.

NOTE: To optionally disable the radio from switching back to its original channel of operation, execute the *no > dfs-rehome* command in the radio interface configuration mode of the access point's profile or device. For more information, see *dfs-rehome*.

NOTE: For radio's having channel selection mode set to ACS, Random, or Fixed adaptivity timeout can be configured in the access point's radio interface mode. For more information, see *adaptivity*.

On the other hand, if the radio's channel selection mode is set to Smart or ACS, once adaptivity or DFS is triggered, the channel is avoided until the avoidance-time, specified here, expires. Once the evacuation period has expired, the channel is free for use by both Smart-RF and ACS.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
avoidance-time [adaptivity|dfs] <30-3600>
```

Parameters

- `avoidance-time [adaptivity|dfs] <30-3600>`

avoidance-time [adaptivity|dfs]	Configures the time for which a channel is avoided after dfs or adaptivity is triggered • adaptivity – Sets the time, in minutes, for which a radio avoids an adaptivity-regulated channel detected with interference • dfs – Sets the time, in minutes, for which a radio avoids a DFS-regulated channel detected with radar • <30-3600> – Specify a value from 30 - 3600 minutes. The default for both parameters is 90 minutes.

Example

```
nx4500-5CFA2B(config-smart-rf-policy-test)#avoidance-time adaptivity 200

nx4500-5CFA2B(config-smart-rf-policy-test)#avoidance-time dfs 300

nx4500-5CFA2B(config-smart-rf-policy-test)#show context
smart-rf-policy test
 avoidance-time dfs 300
 avoidance-time adaptivity 200
nx4500-5CFA2B(config-smart-rf-policy-test)#

nx4500-5CFA2B(config-smart-rf-policy-test)#no avoidance-time adaptivity

nx4500-5CFA2B(config-smart-rf-policy-test)#show context include-factory | include
avoidance-time
 avoidance-time dfs 300
 avoidance-time adaptivity 90
nx4500-5CFA2B(config-smart-rf-policy-test)#
```

Related Commands

no	Reverts the DFS/adaptivity regulated channel avoidance time to default (90 minutes)

19.1.4 channel-list

smart-rf-policy

Assigns a list of channels, for the selected frequency, used in Smart RF scans

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
channel-list [2.4GHz|5GHz] <WORD>
```

Parameters

- `channel-list [2.4GHz|5GHz] <WORD>`

2.4GHz <WORD>	Assigns a channel list for the 2.4 GHz band • <WORD> – Specify a comma separated list of channels
5GHz <WORD>	Assigns a channel list for the 5.0 GHz band • <WORD> – Specify a comma separated list of channels

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#channel-list 2.4GHz 1,12

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Removes the channel list for the selected frequency

19.1.5 channel-width

smart-rf-policy

Selects the channel width for Smart RF configuration

NOTE: In addition to 20 MHz and 40 MHz, AP82XX also provides support for 80 MHz channels.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
channel-width [2.4GHz|5GHz]

channel-width 2.4GHz [20MHz|40MHz|auto]
channel-width 5GHz [20MHz|40MHz|80MHz|auto]
```

Parameters

- `channel-width 2.4GHz [20MHz|40MHz|auto]`

2.4GHz [20MHz|40MHz|auto]	Assigns the channel width for the 2.4 GHz band • 20MHz – Assigns the 20 MHz channel width. This is the default setting. • 40MHz – Assigns the 40 MHz channel width • auto – Assigns the best possible channel in the 20 MHz or 40 MHz channel width

- `channel-width 5GHz [20MHz|40MHz|auto]`

5GHz [20MHz|40MHz|80MHz|auto]	Assigns the channel width for the 5.0 GHz band • 20MHz – Assigns the 20 MHz channel width • 40MHz – Assigns the 40 MHz channel width. This is the default setting. • 80MHz – Assigns the 80 MHz channel width (supported only on AP8232) • auto – Assigns the best possible channel in the 20 MHz, 40 MHz, or 80 MHz channel width

Usage Guidelines

The 20/40 MHz operation allows the access point to receive packets from clients using 20 MHz, and transmit using 40 MHz. This mode is supported for 802.11n users on both the 2.4 GHz and 5.0 GHz radios. If an 802.11n user selects two channels (a primary and secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select *auto* to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#channel-width 5GHz auto

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Resets channel width for the selected frequency to its default

19.1.6 coverage-hole-recovery

smart-rf-policy

Enables recovery from coverage hole errors detected by Smart RF. Use this command to configure the coverage hole recovery settings.

When coverage hole recovery is enabled, on detection of a coverage hole, Smart RF first determines the power increase needed based on the *signal-to-noise ratio* (SNR) for a client as seen by the access point radio. If a client's SNR is above the specified threshold, the transmit power is increased until the SNR falls below the threshold.

NOTE: The coverage-hole-recovery parameters can be modified only if the sensitivity level is set to 'custom'. For more information, see *sensitivity*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
coverage-hole-recovery {client-threshold|coverage-interval|interval|snr-threshold}

coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}

coverage-hole-recovery {coverage-interval|interval} [2.4GHz|5GHz] <1-120>

coverage-hole-recovery {snr-threshold [2.4Ghz|5Ghz] <1-75>}
```

Parameters

- `coverage-hole-recovery {client-threshold [2.4GHz|5GHz] <1-255>}`

client-threshold	Optional. Specifies the minimum number of clients associated to a radio in order to trigger coverage hole recovery.
2.4GHz <1-255>	Specifies the minimum number of clients on the 2.4 GHz band • <1-255> – Sets a value from 1 - 255. The default is 1.
5GHz <1-255>	Specifies the minimum number of clients on the 5.0 GHz band • <1-255> – Sets a value from 1 - 255. The default is 1.

- `coverage-hole-recovery {coverage-interval|interval} [2.4GHz|5GHz] <1-120>`

coverage-interval	Optional. Specifies the interval between the discovery of a coverage hole and the initiation of coverage hole recovery
interval	Optional. Specifies the interval at which coverage hole recovery is performed even before a coverage hole is detected

2.4GHz <1-120>	The following keywords are common to the 'coverage-interval' and 'interval' parameters: • 2.4GHz <1-120> – Specifies the coverage hole recovery interval on the 2.4 GHz band • <1-120> – Specify a value from 1 - 120 seconds. **Note:** coverage-interval – The default is 10 seconds. **Note:** interval – The default is 30 seconds.
5GHz <1-120>	The following keywords are common to the 'coverage-interval' and 'interval' parameters: • 5GHz <1-120> – Specifies a coverage hole recovery interval on the 5.0 GHz band • <1-120> – Specify a value from 1 - 120 seconds. **Note:** coverage-interval – The default is 10 seconds. **Note:** interval – The default is 30 seconds.

- `coverage-hole-recovery` *`{snr-threshold}`* `[2.4Ghz|5Ghz] <1-75>`

snr-threshold	Optional. Specifies the SNR threshold. This value is the SNR threshold for an associated client as seen by its associated AP radio. When the SNR threshold is exceeded, the radio increases its transmit power to increase coverage for the associated client.
2.4GHz <1-75>	Specifies SNR threshold on the 2.4 GHz band • <1-75> – Sets a value from 1 dB - 75 dB. The default is 20 dB.
5GHz <1-75>	Specifies SNR threshold on the 5.0 GHz band • <1-75> – Sets a value from 1 - 75. The default is 20 dB.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#coverage-hole-recovery snr-threshold
5GHz 1

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 coverage-hole-recovery snr-threshold 5GHz 1
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Disables recovery from coverage hole errors

19.1.7 enable

smart-rf-policy

Enables a Smart RF policy

Use this command to enable this Smart RF policy. Once enabled, the policy can be assigned to a RF Domain supporting a network.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
enable
```

Parameters

None

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#enable
```

Related Commands

no	Disables a Smart RF policy

19.1.8 group-by

smart-rf-policy

Enables grouping of APs on the basis of their location in a building (floor) or an area

Within a large RD Domain, grouping of APs (within an area or on the same floor in a building) facilitates statistics gathering and troubleshooting.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
group-by [area|floor]
```

Parameters

- `group-by [area|floor]`

area	Groups radios based on their area of location
floor	Groups radios based on their floor location Both options are disabled by default.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#group-by floor

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 coverage-hole-recovery snr-threshold 5GHz 1
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Removes Smart RF group settings

19.1.9 interference-recovery

smart-rf-policy

Enables interference recovery from neighboring radios and other sources of WiFi and non-WiFi interference. Interference is the excess noise detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interfering sources by monitoring the noise levels and other RF parameters on an access point radio's current channel. When a noise threshold is exceeded, Smart RF selects an alternative channel with less interference. To avoid channel flapping a hold timer is defined, which disables interference avoidance for a specific period of time upon detection. Interference recovery is enabled by default.

NOTE: The interference-recovery parameters can be modified only if the sensitivity level is set to 'custom'. For more information, see *sensitivity*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
interference-recovery {channel-hold-time|channel-switch-delta|client-threshold|
   interference|neighbor-offset|noise|noise-factor}

interference-recovery {channel-switch-delta [2.4GHz|5GHZ] <5-35>}

interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>|
   interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}
```

Parameters

- `interference-recovery {channel-switch-delta [2.4GHz|5GHZ] <5-35>}`

channel-switch-delta	Optional. Configures a threshold value for the difference between interference levels on the current channel and the prospective channel needed to trigger a channel change. If the difference in noise levels on the current channel and the prospective channel is below the configured threshold, the channel is not changed.
[2.4GHz|5GHz]	Selects the band • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<5-35>	Specifies the threshold value for the difference between the current and prospective channel interference levels • <5-35> – Sets a value from 5 dBm - 35 dBm. The default setting is 20 dBm for both 2.4 GHz and 5.0 GHz bands.

- `interference-recovery {channel-hold-time <0-86400>|client-threshold <1-255>| interference|neighbor-offset <3-10>|noise|noise-factor <1.0-3.0>}`

channel-hold-time <0-86400>	Optional. Defines the minimum time between two channel change recoveries • <0-86400> – Sets the time, in seconds, between channel change assignments based on interference or noise. The default is 7,200 seconds.

client-threshold <1-255>	Optional. Specifies client thresholds needed to avoid channel change. If the specified threshold number of clients are connected to a radio, the radio avoids changing channels even if the Smart RF master determines that a channel change is required. • <1-255> – Sets the number of clients from 1 - 255. The default is 50.
interference	Optional. Considers external interference values to perform interference recovery. This feature allows the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default.
neighbor-offset <3-10>	Optional. Configures a noise factor value, which is taken into consideration when switching channels to avoid interference from neighboring access points. Smart RF enabled access points consider the difference in noise between candidate channels. • <3-10> – Specify a noise factor value from 3 - 10.
noise	Optional. Considers noise values to perform interference recovery. This feature allows the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported devices can change their channel and move to a cleaner channel. This feature is enabled by default.
noise-factor <1.0-3.0>	Optional. Configures additional noise factor (the level of network interference detected) for non WiFi interference • <1.0-3.0> – Specify the noise factor from 1.0 - 3.0. The default is 1.50.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#interference-recovery channel-switch-
delta 5GHz 5

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 interference-recovery channel-switch-delta 5GHz 5
 coverage-hole-recovery snr-threshold 5GHz 1
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Disables recovery from excessive noise and interference

19.1.10 neighbor-recovery

smart-rf-policy

Enables recovery from errors due to faulty neighboring radios. Enabling neighbor recovery ensures automatic recovery from failed radios within the radio coverage area. Smart RF instructs neighboring access points to increase their transmit power to compensate for the failed radio. Neighbor recovery is enabled by default when the sensitivity setting is medium.

NOTE: The neighbor-recovery parameters can be modified only if the sensitivity level is set to 'custom'. For more information, see *sensitivity*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
neighbor-recovery {dynamic-sampling|power-hold-time|power-threshold}
neighbor-recovery {dynamic-sampling} {retries <1-10>|threshold <1-30>}
neighbor-recovery {power-hold-time <0-3600>}
neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}
```

Parameters

- `neighbor-recovery {dynamic-sampling} {retries <1-10>|threshold <1-30>}`

dynamic-sampling	Optional. Enables dynamic sampling on this Smart RF policy. Dynamic sampling allows you to define how Smart RF adjustments are triggered by locking the 'retry' and 'threshold' values. Dynamic sampling is disabled by default.
retries <1-10>	Optional. Specifies the number of retries before allowing a power level adjustments to compensate for a potential coverage hole. • <1-10> – Sets the number of retries from 1 - 10. The default is 3.
threshold <1-30>	Optional. Specifies the minimum number of sample reports before which a power change requires dynamic sampling • <1-30> – Sets the minimum number of reports from 1 - 30. The default is 5.

- `neighbor-recovery {power-hold-time <0-3600>}`

power-hold-time	Optional. Specifies the minimum time, in seconds, between two power changes on a radio during neighbor-recovery
<0-3600>	Sets the time from 0 - 3600 sec. The default is 0 seconds.

- `neighbor-recovery {power-threshold [2.4Ghz|5Ghz] <-85--55>}`

power-threshold	Optional. Specifies the power threshold based on which recovery is performed The 2.4 GHz/5.0 GHz radio uses the value specified here as the maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within its coverage area.
[2.4GHz|5GHz]	Selects the band • 2.4GHz – Selects the 2.4 GHz band • 5GHz – Selects the 5.0 GHz band
<-85--55>	Specify the threshold value • <-85--55> – Sets the power threshold from -85 dBm - -55 dBm. The default is -70 dBm for both the 2.4 GHz and 5.0 GHz bands.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold
2.4GHz
-82

rfs6000-37FABE(config-smart-rf-policy-test)#neighbor-recovery power-threshold
5GHz -65

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 interference-recovery channel-switch-delta 5GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -82
 coverage-hole-recovery snr-threshold 5GHz 1
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Disables recovery from faulty neighbor radios

19.1.11 no

smart-rf-policy

Negates a command or sets its default. When used in the config Smart RF policy mode, the `no` command disables or resets Smart RF settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [area|assignable-power|avoidance-time|channel-list|channel-width|
coverage-hole-recovery|enable|group-by|interference-recovery|neighbor-recovery|
smart-ocs-monitoring]

no area <AREA-NAME> channel-list [2.4GHZ|5GHZ]

no assignable-power [2.4GHZ|5GHZ] [max|min]

no [channel-list|channel-width] [2.4GHZ|5GHZ]

no coverage-hole-recovery [client-threshold|coverage-interval|interval|snr-
threshold] [2.4GHZ|5GHZ]

no avoidance-time [adaptivity|dfs]

no enable

no group-by [area|floor]

no interference-recovery {channel-hold-time|channel-switch-delta [2.4GHZ|5GHZ]|
client-threshold|interference|neighbor-offset|noise|noise-factor}

no neighbor-recovery {dynamic-sampling {retries|threshold}|power-hold-time|
power-threshold [2.4GHZ|5GHZ]}

no smart-rf-monitoring {awareness-override [schedule <1-3>|threshold]|client-
aware [2.4GHZ|5GHZ]|extended-scan-frequency [2.4GHZ|5GHZ]|frequency
[2.4GHZ|5GHZ]|off-channel-duration [2.4GHZ|5GHZ]|power-save-aware
[2.4GHZ|5GHZ]|sample-count [2.4GHZ|5GHZ]|voice-aware [2.4GHZ|5GHZ]}
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or sets its default. When used in the config Smart RF policy mode, the `no` command disables or resets the Smart RF policy settings.

Example

The following example shows the Smart RF policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 assignable-power 5GHz min 8
 assignable-power 5GHz max 20
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 interference-recovery channel-switch-delta 5GHz 5
 neighbor-recovery power-threshold 5GHz -65
 neighbor-recovery power-threshold 2.4GHz -82
 coverage-hole-recovery snr-threshold 5GHz 1
rfs6000-37FABE(config-smart-rf-policy-test)#
rfs6000-37FABE(config-smart-rf-policy-test)#no interference-recovery channel-
switch-delta 5GHz
rfs6000-37FABE(config-smart-rf-policy-test)#no neighbor-recovery power-threshold
2.4GHz
rfs6000-37FABE(config-smart-rf-policy-test)#no neighbor-recovery power-threshold
5GHz
rfs6000-37FABE(config-smart-rf-policy-test)#no assignable-power 5GHz min
rfs6000-37FABE(config-smart-rf-policy-test)#no assignable-power 5GHz max
```

The following example shows the Smart RF policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 coverage-hole-recovery snr-threshold 5GHz 1
rfs6000-37FABE(config-smart-rf-policy-test)#
```

19.1.12 sensitivity

smart-rf-policy

Configures Smart RF sensitivity level. The sensitivity level determines Smart RF scanning and sampling aggressiveness. For example, a low sensitivity level indicates a less aggressive Smart-RF policy. This translates to fewer samples taken during off-channel scanning and short off-channel durations. When the sensitivity level is set to high, Smart-RF collects more samples, and remains off-channel longer.

The Smart RF sensitivity level options include low, medium, high, and custom. Medium, is the default setting. The custom option allows an administrator to adjust the parameters and thresholds for interference recovery, coverage hole recovery, and neighbor recovery. However, the low, medium, and high settings still allow utilization of these features.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
sensitivity [custom|high|low|medium]
```

Parameters

- `sensitivity [custom|high|low|medium]`

sensitivity	Configures Smart RF sensitivity levels. The options available are: custom, high, low, and medium.
custom	Enables custom interference recovery, coverage hole recovery, and neighbor recovery as additional Smart RF options
high	High sensitivity
low	Low sensitivity
medium	Medium sensitivity. This is the default setting.

Usage Guidelines

To enable the *power* and *channel setting* parameters, set *sensitivity* to *custom* or *medium*.

To enable the *monitoring* and *scanning* parameters, set *sensitivity* to *custom*.

To enable the *neighbor recovery*, *interference* and *coverage hole recovery* parameters, set *sensitivity* to *custom*.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#sensitivity high

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity high
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring sample-count 2.4GHz 3
 --More--
rfs6000-37FABE(config-smart-rf-policy-test)#
```

19.1.13 smart-ocs-monitoring

smart-rf-policy

Applies smart *Off Channel Scanning* (OCS) instead of dedicated detectors

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
smart-ocs-monitoring {awareness-override|client-aware|extended-scan-frequency|
frequency|off-channel-duration|power-save-aware|sample-count|tx-load-aware|
voice-aware}

smart-ocs-monitoring {awareness-override [schedule|threshold]}
smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME>
<DAY>}

smart-ocs-monitoring {awareness-override threshold <10-10000>}

smart-ocs-monitoring {client-aware [2.4GHz|5GHz] <1-255>}

smart-ocs-monitoring {extended-scan-frequency [2.4GHz|5GHz] <0-50>}

smart-ocs-monitoring {frequency [2.4GHz|5GHz] <1-120>}

smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}

smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz] [disable|dynamic|strict]}

smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}

smart-ocs-monitoring {tx-load-aware [2.4GHz|5GHz] <1-100>}

smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}
```

Parameters

```
• smart-ocs-monitoring {awareness-override schedule <1-3> <START-TIME> <END-TIME>
<DAY>}
```

awareness-override	Optional. Use this parameter to configure client awareness settings overrides

schedule <1-3> <START-TIME> <END-TIME> {<DAY>}	Configures a time and day schedule when awareness settings are overridden
	• <1-3> – Sets the awareness override schedule index. A maximum of three overrides can be configured.
	  • <START-TIME> – Sets the override start time in HH:MM format
	  • <END-TIME> – Sets the override end time in HH:MM format
	  • DAY – Optional. Set the day when the override is active. Use one of the following formats:
	  • all – Override is active on all days
	  • sun – Override is active only on Sundays
	  • mon – Override is active only on Mondays
	Contd..

	• tue – Override is active only on Tuesdays • wed – Override is active only on Wednesdays • thu – Override is active only on Thursdays • fri – Override is active only on Fridays • sat – Override is active only on Saturdays

- `smart-ocs-monitoring` *`{awareness-override threshold <10-10000>}`*

awareness-override threshold <10-10000>	Optional. Use this parameter to configure client awareness settings overrides • threshold – Specifies the threshold after which client awareness settings are overridden. When the specified threshold is reached, awareness settings are overridden. • <10-10000> – Specify a threshold value from 10 -10000. The default is 10.

- `smart-ocs-monitoring` *`{client-aware [2.4GHz|5GHz] <1-255>}`*

client-aware	Optional. Enables client aware scanning on this Smart RF policy Use this parameter to configure a client threshold number. When the number of clients connected to a radio equals this threshold number, the radio avoids channel scanning. This feature is disabled by default.
2.4GHz <1-255>	Enables client aware scanning on the 2.4 GHz band Avoids radio scanning when a specified minimum number of clients are present • <1-255> – Sets the minimum number of clients from 1 - 255. The default is 1 client.
5GHz <1-255>	Enables client aware scanning on the 5.0 GHz band Avoids radio scanning when a specified minimum number of clients are present • <1-255> – Sets the minimum number of clients from 1 - 255. The default is 1 client.

- `smart-ocs-monitoring` *`{extended-scan-frequency [2.4GHz|5GHz] <0-50>}`*

extended-scan-frequency	Optional. Enables an extended scan, as opposed to a neighbor only scan, on this Smart RF policy. This is the frequency radios use to scan for non-peer radios.
2.4GHz <0-50>	Enables extended scan on the 2.4 GHz band • <0-50> – Sets the number of trails from 0 - 50. The default is 5.
5GHz <0-50>	Enables extended scan on the 5.0 GHz band • <0-50> – Sets the number of trails from 0 - 50. The default is 5.

- `smart-ocs-monitoring` *`{frequency [2.4GHz|5GHz] <1-120>}`*

frequency	Optional. Specifies the scan frequency. This is the frequency, in seconds, in which smart-ocs-monitoring changes channels for an off channel scan.
2.4GHz <1-120>	Selects the 2.4 GHz band • <1-120> – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.
5GHz <1-120>	Selects the 5.0 GHz band • <1-120> – Sets a scan frequency from 1 - 120 sec. The default is 6 seconds.

- `smart-ocs-monitoring {off-channel-duration [2.4GHz|5GHz] <20-150>}`

off-channel-duration	Optional. Specifies the duration to scan off channel This is the duration access point radios use to monitor devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within a RF Domain.
2.4GHz <20-150>	Selects the 2.4 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 - 150 msec. The default is 50 milliseconds.
5GHz <20-150>	Selects the 5.0 GHz band (in milliseconds) • <20-150> – Sets the off channel duration from 20 - 150 msec. The default is 50 milliseconds.

- `smart-ocs-monitoring {power-save-aware [2.4GHz|5GHz] [disable|dynamic|strict]}`

power-save-aware	Optional. Enables power save awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. This setting allows Smart RF to detect power save clients and take them into consideration when performing off channel scans. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio.
2.4GHz [disable|dynamic|strict]	Sets power save awareness scanning mode on the 2.4 GHz band • disable – Disables power save awareness scanning • dynamic – Dynamically avoids scanning based on traffic for power save (PSP) clients • strict – Strictly avoids scanning when PSP clients are present The default is dynamic.
5GHz [disable|dynamic|strict]	Sets power save awareness scanning mode on the 5.0 GHz band • disable – Disables power save awareness scanning • dynamic – Dynamically avoids scanning based on traffic for PSP clients • strict – Strictly avoids scanning when PSP clients are present The default is dynamic.

- `smart-ocs-monitoring {sample-count [2.4GHz|5GHz] <1-15>}`

sample-count	Optional. Specifies the number of samples to collect before reporting an issue to the Smart RF master
2.4GHz <1-15>	Selects the 2.4 GHz band • <1-15> – Specifies the number of samples to collect from 1 - 15. The default is 10.
5GHz <1-15>	Selects the 5.0 GHz band • <1-15> – Specifies the number of samples to collect from 1 - 15. The default is 5.

- `smart-ocs-monitoring {tx-load-aware [2.4GHz|5GHz] <1-100>}`

tx-load-aware	Optional. Specifies a transmit load percentage that serves as a threshold before scanning is avoided for an access point's 2.4 GHz or 5.0 GHz band. This option is disabled for both 2.4 GHz and 5.0 GHz bands.

2.4GHz <1-100>	Selects the 2.4 GHz band • <1-100> – Specify a transmit load percentage from 1 - 100%. When enabled, the default is 1%.
5GHz <1-100>	Selects the 5.0 GHz band • <1-100> – Specify a transmit load percentage from 1 - 100%. When enabled, the default is 1%.

- `smart-ocs-monitoring {voice-aware [2.4GHz|5GHz] [disable|dynamic|strict]}`

voice-aware	Optional. Enables voice awareness scanning mode on this Smart RF policy. The options are: disable, dynamic, and strict. Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio.
2.4GHz [disable|dynamic|strict]	Specifies the scanning mode on the 2.4 GHz band • disable – Disables voice awareness scanning • dynamic – Dynamically avoids scanning based on traffic for voice clients • strict – Strictly avoids scanning when voice clients are present **Note:** The default is dynamic.
5GHz [disable|dynamic|strict]	Specifies the scanning mode on the 5.0 GHz band • disable – Disables voice awareness scanning • dynamic – Dynamically avoids scanning based on traffic for voice clients • strict – Strictly avoids scanning when voice clients are present. **Note:** The default is dynamic.

Example

```
rfs6000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring extended-scan-
frequency 2.4GHz 9
rfs6000-37FABE(config-smart-rf-policy-test)#smart-ocs-monitoring sample-count
2.4GHz 3

rfs6000-37FABE(config-smart-rf-policy-test)#show context
smart-rf-policy test
 area test channel-list 2.4GHz 1,2,3
 group-by floor
 sensitivity custom
 channel-list 2.4GHz 1,12
 channel-width 5GHz auto
 smart-ocs-monitoring off-channel-duration 2.4GHz 25
 smart-ocs-monitoring frequency 5GHz 3
 smart-ocs-monitoring frequency 2.4GHz 3
 smart-ocs-monitoring sample-count 5GHz 3
 smart-ocs-monitoring sample-count 2.4GHz 3
 smart-ocs-monitoring extended-scan-frequency 5GHz 0
 smart-ocs-monitoring extended-scan-frequency 2.4GHz 9
 root-recovery root-path-metric-threshold 800
--More--
rfs6000-37FABE(config-smart-rf-policy-test)#
```

Related Commands

no	Disables off channel monitoring

20 WIPS-POLICY

This chapter summarizes the *Wireless Intrusion Protection Systems* (WIPS) policy commands in the CLI command structure.

WIPS is an additional measure of security designed to continuously monitor the network for threats and intrusions. Along with wireless VPNs, encryptions, and authentication policies WIPS enhances the security of a WLAN.

The WIPS policy enables detection of intrusions and threats that a managed network is likely to encounter. However, the WIPS policy does not include threat mitigation configurations. These intrusions and threats are available within the WIPS policy configuration mode as pre configured, fixed events. Each event consists of a set of frames or anomalies that may be harmful to the managed network. You can enable/disable various aspects of each individual event.

Events are broadly grouped into the following three categories:

- Excessive/Thresholdable events: These events detect DOS attacks, like excessive deauths, EAP floods, etc. Threshold limits for such events can be configured for *mobile units* (MU) and radios. Once these threshold limits are exceeded, an event is triggered. Stations triggering an event are usually filtered. You can configure a filter ageout specifying the time for which the station, triggering the event, is filtered. However, the filter ageout only applies when the MU-threshold is exceeded. When radio threshold is reached, the system raises a warning about the same and updates event history with event details.
- Station/MU anomalies: These events are triggered when a MU performs suspicious activities that can compromise the security and stability of the managed network. You can configure a filter ageout, similar to the above class of events, to filter the station triggering such events.
- AP/neighbor anomalies: These events are triggered when an AP or neighbor sends suspicious frames. The system cannot filter APs or neighbors triggering such events. However, the system warns you about such attacks, allowing you to take further actions against such APs and neighbors.

In addition to event monitoring configuration, the WIPS policy allows you to configure a list of signatures. Unlike events, signatures are not fixed. You are free to define your own signatures based on a specific set of parameters. A signature is a rule, consisting of a set of fields to match and a corresponding set of actions in case of a match. By default, whenever a signature is matched an event log is triggered. This event log is similar to the one triggered upon an event. In addition to an event log, you can also configure other actions. Signatures have all the features supported by events. In fact most events are internally implemented as signatures.

Signature rules are of the following three types:

- ssid, ssid length rule: This signature matches a specified SSID or SSID length. It is mandatory to configure the frame type to match for this signature. When configured, only frame types allowed are beacons, probe requests, and probe responses. Example rule: ssid : AirJack and frame type beacon : Signature for AirJack attack.
- payload rule: This signature matches a particular payload at a particular frame offset. You can restrict these matches based on frame type. Example rule: Payload : 0x00601d Offset 3 : Netstumbler
- address-match rule: This signature matches one or more address fields. The address fields supported are BSSID, source-MAC, and destination-MAC. You can also specify frame types to

match. The frame types supported are assoc, auth, beacon, data, deauth, disassoc, mgmt, probe-request, and probe-response.

A WIPS policy, once configured, has to be attached to a RF Domain to take effect. Multiple WIPS policies can be configured at the same time, but only one policy can be attached to a given RF Domain at any time.

NOTE: To attach a WIPS policy to a RF Domain, in the RF Domain configuration mode, execute the *use > wips-policy <WIPS-POLICY-NAME>* command. For more information, see *use*.

NOTE: With this most recent release, AP7522 and AP7532 model Access Points can provide enhanced sensor support. AP7522 and AP7532 sensors can send data from off-channel-scans while in radio-share promiscuous/inline mode, in addition to the on-channel data captured in radio-share mode. ADSP uses the off-channel-scan data (in addition to the on-channel data) to monitor for rogue intrusions and trigger alarms. OTA Termination is triggered from ADSP to the appropriate radio-share AP to initiate termination.

NOTE: AP7522 and AP7532 models also support shared part-time scanning using WIPS in WiNG (using off-channel-scans) and no ADSP. WIPS on WiNG was enhanced to add rogue detection/classification (wired side detection based of MAC Address Offset) and *over-the-air* (OTA) termination for AP7522 and AP7532 deployments.

Use the (config) instance to configure WIPS policy commands. To navigate to the WIPS policy instance, use the following commands:

```
<DEVICE>(config)#wips-policy <POLICY-NAME>

rfs6000-37FABE(config)#wips-policy test
rfs6000-37FABE(config-wips-policy-test)#?
Wips Policy Mode commands:
  ap-detection                Rogue AP detection
  enable                      Enable this wips policy
  event                       Configure an event
  history-throttle-duration   Configure the duration for which event duplicates
                              are not stored in history
  interference-event          Specify events which will contribute to smart-rf
                              wifi interference calculations
  no                          Negate a command or set its defaults
  signature                   Signature to configure
  use                         Set setting to use
  clrscr                      Clears the display screen
  commit                      Commit all changes made in this session
  do                          Run commands from Exec mode
  end                         End current mode and change to EXEC mode
  exit                        End current mode and down to previous mode
  help                        Description of the interactive help system
  revert                      Revert changes
  service                     Service Commands
  show                        Show running system information
  write                       Write running configuration to memory or terminal
```

```
rfs6000-37FABE(config-wips-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

20.1 wips-policy

- *WIPS-POLICY*

The following table summarizes WIPS policy configuration commands:

Table 20.1 *WIPS-Policy-Config Commands*

Command	Description	Reference
ap-detection	Defines the WIPS AP detection configuration	*page 20-5*
enable	Enables a WIPS policy	*page 20-7*
event	Configures events	*page 20-8*
history-throttle-duration	Configures the duration event duplicates are omitted from the event history	*page 20-12*
interference-event	Specifies events contributing to the Smart RF WiFi interference calculations	*page 20-13*
no	Negates a command or sets its default	*page 20-14*
signature	Configures a WIPS policy signature and enters its configuration mode	*page 20-16*
use	Defines a WIPS policy settings	*page 20-33*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

20.1.1 ap-detection

wips-policy

Enables the detection of unauthorized or unsanctioned APs. Unauthorized APs are untrusted access points connected to an access point managed network. These untrusted APs accept wireless client associations. It is important to detect such rogue APs and declare them unauthorized. Rogue AP detection is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ap-detection {ageout|air-termination|interferer-threshold|recurring-event-interval|wait-time}

ap-detection {ageout <30-86400>|interferer-threshold <-100--10>|recurring-event-interval <0-10000>|wait-time <10-600>}

ap-detection air-termination {allow-channel-switch|mode [auto|manual]}
```

Parameters

```
• ap-detection {ageout <30-86400>|interferer-threshold <-100--10>|recurring-event-interval <0-10000>|wait-time <10-600>}
```

ap-detection	Enables detection of unauthorized or unsanctioned APs
ageout <30-86400>	Optional. Configures the unauthorized AP ageout interval. The WIPS policy uses this value to ageout unauthorized APs. • <30-86400> – Sets an ageout interval from 30 - 86400 seconds. The default is 5 minutes (300 seconds).
recurring-event-interval <0-10000>	Configures recurring event interval help of unauthorized APs • <0-10000> – Configures the recurring interval between 0 - 10000 seconds. The default is 300 seconds.
interferer-threshold <-100--10>	Configures RSSI threshold value to determine if an unsanctioned ap is an interferer or not • <-100--10> – Configures the rssi threshold between -100 - -10 dBm. The default is -75 dBm.
wait-time <10-600>	Optional. Configures the wait time before a detected AP is declared as unauthorized and potentially removed • <10-600> – Sets a wait time from 10 - 600 seconds. The default is 1 minute (60 seconds).

- `ap-detection air-termination {allow-channel-switch|mode [auto|manual]}`

ap-detection	Enables detection of unauthorized or unsanctioned APs
air-termination {allow-channel-switch| mode [auto|manual]}	Enables air termination of unauthorized APs. This option is disabled by default. • allow-channel-switch – Optional. Allows channel switch of unauthorized APs based on the channel mode. This option is disabled by default. • mode [auto|manual] – Optional. Select the mode as auto or manual to configure. The default setting is manual.

Example

```
rfs6000-37FABE(config-wips-policy-test)#ap-detection wait-time 15
rfs6000-37FABE(config-wips-policy-test)#ap-detection age-out 50

rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 ap-detection-age-out 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#

nx9500-6C8809(config-wips-policy-test)#ap-detection recurring-event-interval 10

nx9500-6C8809(config-wips-policy-test)#show context
wips-policy test
 ap-detection recurring-event-interval 10
nx9500-6C8809(config-wips-policy-test)#
```

Related Commands

no	Resets unauthorized or unsanctioned AP detection settings to default

20.1.2 enable

wips-policy

Enables this WIPS policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
enable
```

Parameters

None

Example

```
rfs6000-37FABE(config-wips-policy-test)#enable
rfs6000-37FABE(config-wips-policy-test)#
```

Related Commands

no	Disables a WIPS policy

20.1.3 event

wips-policy

Configures events, filters and threshold values for this WIPS policy. Events are grouped into three categories, AP anomaly, client anomaly, and excessive. WLANs are baselined for matching criteria. Any deviation from this baseline is considered an anomaly and logged as an event.

NOTE: By default all event monitoring is disabled.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]

event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
unencrypted-wired-leakage|wireless-bridge]

event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|
fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|
identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|
non-conforming-data|wellenreiter] {filter-ageout <0-86400>}

event enable-all-events

event excessive [80211-replay-check-failure|aggressive-scanning|auth-server-
failures|decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|
dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-
station] {filter-ageout <0-86400>|threshold-client <0-65535>|threshold-radio <0-
65535>}
```

Parameters

```
• event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
impersonation-attack|null-probe-response|transmitting-device-using-invalid-mac|
unencrypted-wired-leakage|wireless-bridge]
```

ap-anomaly	Enables AP anomaly event tracking An AP anomaly event refers to suspicious frames sent by neighboring APs. An administrator enables the filtering of each listed event and sets the thresholds for the generation of event notification and filtering.
ad-hoc-violation	Tracks ad-hoc network violations
airjack	Tracks AirJack attacks
ap-ssid-broadcast-in-beacon	Tracks AP SSID broadcasts in beacon events
asleap	Tracks ASLEAP attacks. These attacks break *Lightweight Extensible Authentication Protocol* (LEAP) passwords
impersonation-attack	Tracks impersonation attacks. These are also referred to as spoofing attacks, where the attacker assumes the address of an authorized device.

null-probe-response	Tracks null probe response attacks
transmitting-device-using-invalid-mac	Tracks the transmitting device using an invalid MAC attacks
unencrypted-wired-leakage	Tracks unencrypted wired leakage
wireless-bridge	Tracks *wireless bridge* (WDS) frames

- `event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|non-conforming-data|wellenreiter]` *`{filter-ageout <0-86400>}`*

client-anomaly	Enables client anomaly event tracking These are suspicious events performed by wireless clients compromising the security of the network. An administrator can enable or disable filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action applied.
dos-broadcast-deauth	Tracks DoS broadcast deauthentication events
fuzzing-all-zero-macs	Tracks Fuzzing: All zero MAC addresses observed
fuzzing-invalid-frame-type	Tracks Fuzzing: Invalid frame type detected
fuzzing-invalid-mgmt-frames	Tracks Fuzzing: Invalid management frame detected
fuzzing-invalid-seq-num	Tracks Fuzzing: Invalid sequence number detected
identical-src-and-dest-addr	Tracks identical source and destination addresses detection
invalid-8021x-frames	Tracks Fuzzing: Invalid 802.1x frames detected
netstumbler-generic	Tracks Netstumbler (v3.2.0, 3.2.3, 3.3.0) events
non-conforming-data	Tracks non conforming data packets
wellenreiter	Tracks Wellenreiter events
filter-ageout <0-86400>	The following keywords are common to all of the above client anomaly events: • filter-ageout <0-86400> – Optional. Configures the filter expiration interval in seconds • <0-86400> – Sets the filter ageout interval from 0 - 86400 seconds. The default is 0 seconds. **Note:** For each violation define a filter time in seconds, which determines how long the packets (received from an attacking device) are ignored once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed. The filter ageout value is applicable across the entire RF Domain using this WIPS policy. If an MU is detected performing an attack and is filtered by one of the APs, the information is passed on to all APs and controllers within the RF Domain through the domain manager. Consequently the MU is filtered, for the specified period of time, across all devices.

- `event enable-all-events`

enable-all-events	Enables tracking of all intrusion events (client anomaly and excessive events)

```
• event excessive [80211-replay-check-failure|aggressive-scanning|auth-server-
failures|decryption-failures|dos-assoc-or-auth-flood|dos-eapol-start-storm|dos-
unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|frames-from-unassoc-station]
{filter-ageout [<0-86400>]|threshold-client [<0-5535>]|threshold-radio <0-65535>}
```

excessive	Enables the tracking of excessive events. Excessive events are actions performed continuously and repetitively. These events can impact the performance of the controller managed network. DoS attacks come under this category.
80211-replay-check-failure	Tracks 802.11replay check failure
aggressive-scanning	Tracks aggressive scanning events
auth-server-failures	Tracks failures reported by authentication servers
decryption-failures	Tracks decryption failures
dos-assoc-or-auth-flood	Tracks DoS association or authentication floods
dos-eapol-start-storm	Tracks DoS EAPOL start storms
dos-unicast-deauth-or-disassoc	Tracks DoS dissociation or deauthentication floods
eap-flood	Tracks EAP floods
eap-nak-flood	Tracks EAP NAK floods
frames-from-unassoc-station	Tracks frames from unassociated clients
filter-ageout <0-86400>	The following keywords are common to all excessive events: • filter-ageout <0-86400> – Optional. Configures a filter expiration interval in seconds. It sets the duration for which the client is filtered. The client is added to a ACL as a special entry and frames received from this client are dropped. • <0-86400> – Sets a filter ageout interval from 0 - 86400 seconds. The default is 0 seconds. **Note:** This value is applicable across the RF Domain. If a client is detected performing an attack and is filtered by one of the APs, the information is passed to the domain controller. The domain controller then propagates this information to all APs and wireless controllers in the RF Domain.
threshold-client <0-65535>	The following keywords are common to all excessive events: • threshold-client <0-65535> – Optional. Configures a client threshold value after which the filter is triggered and an event is recorded • <0-65535> – Sets a wireless client threshold value from 0 - 65535 seconds
threshold-radio <0-65535>	The following keywords are common to all excessive events: • threshold-radio <0-65535> – Optional. Configures a radio threshold value after which the filter is triggered and an event is recorded • <0-65535> – Sets a radio threshold value from 0 - 65535 seconds

Example

```
rfs6000-37FABE(config-wips-policy-test)#event excessive 80211-replay-check-
failure filter-ageout 9 threshold-client 8 threshold-radio 99

rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#
```

Related Commands

no	Disables WIPS policy events tracking

20.1.4 history-throttle-duration

wips-policy

Configures the duration event duplicates are omitted from the event history

The system maintains a history of all events that have occurred, on each device, within a RF Domain. Sometimes an event occurs for a prolonged period of time and tends to fill up the event history list. In such a scenario, duplicate information added to the event history list can be throttled for a specified period of time. Once this period is over, duplicate entries are once again allowed.

Event history statistics are periodically sent to the domain manager, which can be queried to ascertain the general health of the domain.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
history-throttle-duration <30-86400>
```

Parameters

- `history-throttle-duration <30-86400>`

history-throttle-duration <30-86400>	Configures the duration event duplicates are omitted from the event history • <30-86400> – Sets a value from 30 - 86400 seconds. The default is 120 seconds.

Example

```
rfs6000-37FABE(config-wips-policy-test)#history-throttle-duration 77

rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#
```

Related Commands

no	Resets the history throttle duration to its default (120 seconds)

20.1.5 interference-event

wips-policy

Specifies events contributing to the Smart RF WiFi interference calculations

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
interference-event [non-conforming-data|wireless-bridge]
```

Parameters

- `interference-event [non-conforming-data|wireless-bridge]`

non-conforming-data	Considers non conforming data packets when calculating Smart RF interference
wireless-bridge	Considers Wireless Bridge (WDS) frames when calculating Smart RF interference

Example

```
rfs6000-37FABE(config-wips-policy-test)#interference-event non-conforming-data

rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 interference-event non-conforming-data
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#
```

Related Commands

no	Disables this WIPS policy signature as a Smart RF interference source

20.1.6 no

wips-policy

Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the `no` command negates or resets filters and thresholds.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [ap-detection|enable|event|history-throttle-duration|interference-event|
signature|use]

no [enable|history-throttle-duration]

no ap-detection {ageout {<LINE-SINK>}|air-termination|interferer-threshold <-100-
-10>|recurring-event-interval <0-10000>wait-time {<LINE-SINK>}}

no event [ap-anomaly|client-anomaly|enable-all-events|excessive]

no event ap-anomaly [ad-hoc-violation|airjack|ap-ssid-broadcast-in-beacon|asleap|
impersonation-attack|null-porbe-response|transmitting-device-using-invalid-mac|
unencrypted-wired-leakage|wireless-bridge]

no event client-anomaly [dos-broadcast-deauth|fuzzing-all-zero-macs|fuzzing-
invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzing-invalid-seq-num|
identical-src-and-dest-addr|invalid-8021x-frames|netstumbler-generic|
non-conforming-data|wellenreiter] {filter-ageout <0-86400>}

no event excessive [80211-replay-check-failure|aggressive-scanning|
auth-server-failures|decryption-failures|dos-assoc-or-auth-flood|
dos-eapol-start-storm|dos-unicast-deauth-or-disassoc|eap-flood|eap-nak-flood|
frames-from-unassoc-station] {filter-ageout <0-86400>|threshold-client <0-65535>|
threshold-radio <0-65535>}

no interference-event [non-conforming-data|wireless-bridge]

no signature <WIPS-SIGNATURE>

no use device-categorization
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or resets configured settings to their default. When used in the config WIPS policy mode, the `no` command negates or resets filters and thresholds.

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example shows the WIPS Policy ‘test’ settings before the ‘no’ commands are executed:

```
rrfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 history-throttle-duration 77
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 event client-anomaly wellenreiter filter-ageout 99
 interference-event non-conforming-data
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#

rfs6000-37FABE(config-wips-policy-test)#no event client-anomaly wellenreiter
filter-ageout 99
rfs6000-37FABE(config-wips-policy-test)#no interference-event non-conforming-data
rfs6000-37FABE(config-wips-policy-test)#no history-throttle-duration
```

The following example shows the WIPS Policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#
```

20.1.7 signature

wips-policy

Attack and intrusion patterns are identified and configured as signatures in a WIPS policy. The WIPS policy compares packets in the network with pre configured signatures to identify threats.

The following table summarizes WIPS policy signature configuration commands:

Table 20.2 *WIPS-Policy-Signature-Config Commands*

signature	Configures a WIPS policy signature and enters its configuration mode	*page 20-17*
signature mode commands	Summarizes WIPS signature configuration mode commands	*page 20-19*

20.1.7.1 signature

signature

Configures a WIPS policy signature. A WIPS signature is the set of parameters or patterns used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
signature <SIGNATURE-NAME>
```

Parameters

- `signature <SIGNATURE-NAME>`

signature <SIGNATURE-NAME>	Configures a WIPS policy signature • <SIGNATURE-NAME> – Enter a name for the WIPS policy signature. The name should not exceed 64 characters.

Example

```
rfs6000-37FABE(config-wips-policy-test)#signature test
rfs6000-37FABE(config-test-signature-test)#

rfs6000-37FABE(config-test-signature-test)#?
Wips Signature Mode commands:
  bssid               Bssid mac address
  dst-mac             Destination mac address
  filter-ageout       Configure filter ageout
  frame-type          Configure frame-type to match
  interference-event  Signature is a smart-rf interference source
  mode                Enable/Disable signature
  no                  Negate a command or set its defaults
  payload             Configure a payload
  src-mac             Source mac address
  ssid-match          Match based on ssid
  threshold-client    Configure client threshold limit
  threshold-radio     Configure radio threshold limit

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

rfs6000-37FABE(config-test-signature-test)#
```

```
rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
  threshold-client 88
  payload 1 pattern test offset 1
 ap-detection-ageout 50
 ap-detection-wait-time 15
rfs6000-37FABE(config-wips-policy-test)#
```

Related Commands

no	Deletes a WIPS policy signature

20.1.7.2 signature mode commands

signature

The following table summarizes WIPS policy signature configuration mode commands:

Table 20.3 *WIPS-Policy-Signature-Mode Commands*

Commands	Description	Reference
bssid	Configures the BSSID MAC address	*page 20-20*
dst-mac	Configures the destination MAC address	*page 20-21*
filter-ageout	Configures the filter ageout interval	*page 20-22*
frame-type	Configures the frame type used for matching	*page 20-23*
interference-event	Configures this WIPS policy signature as the Smart RF interference source	*page 20-24*
mode	Enables the signature mode	*page 20-25*
payload	Configures payload settings	*page 20-26*
src-mac	Configures the source MAC address	*page 20-27*
ssid-match	Configures a match based on SSID	*page 20-28*
threshold-client	Configures the wireless client threshold limit	*page 20-29*
threshold-radio	Configures the radio threshold limit	*page 20-30*
no	Negates a command or sets its default	*page 20-31*

20.1.7.2.1 bssid

signature mode commands

Configures a BSSID MAC address with this WIPS signature for matching

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
bssid <MAC>
```

Parameters

- `bssid <MAC>`

bssid <MAC>	Configures a BSSID MAC address to match • <MAC> – Specify the MAC address.

Example

```
rfs6000-37FABE(config-test-signature-test)#bssid 11-22-33-44-55-66

rfs6000-37FABE(config-test-signature-test)#show context
signature test
bssid 11-22-33-44-55-66
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Disables a WIPS signature BSS ID

20.1.7.2.2 dst-mac

signature mode commands

Configures a destination MAC address for the packet examined for matching

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
dst-mac <MAC>
```

Parameters

- `dst-mac <MAC>`

dst-mac <MAC>	Configures a destination MAC address to match • <MAC> – Specify the destination MAC address.

Example

```
rfs6000-37FABE(config-test-signature-test)#dst-mac 55-66-77-88-99-00

rfs6000-37FABE(config-test-signature-test)#show context
signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Disables a WIPS signature destination MAC address

20.1.7.2.3 filter-ageout

signature mode commands

Configures the filter ageout interval in seconds. This is the duration a client, triggering a WIPS event, is excluded from RF Domain manager radio association.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
filter-ageout <1-86400>
```

Parameters

- `filter-ageout <1-86400>`

filter-ageout <1-86400>	Configures the filter ageout interval from 1 - 86400 seconds

Example

```
rfs6000-37FABE(config-test-signature-test)#filter-ageout 8

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  filter-ageout 8
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Removes the configured filter ageout interval

20.1.7.2.4 frame-type

signature mode commands

Configures the frame type used for matching with this WIPS policy signature

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|reassoc]
```

Parameters

```
• frame-type [all|assoc|auth|beacon|data|deauth|disassoc|mgmt|probe-req|probe-resp|reassoc]
```

frame-type	Configures the frame type used for matching
all	Configures all frame type matching
assoc	Configures association frame matching
auth	Configures authentication frame matching
beacon	Configures beacon frame matching
data	Configures data frame matching
deauth	Configures deauthentication frame matching
disassoc	Configures disassociation frame matching
mgmt	Configures management frame matching
probe-req	Configures probe request frame matching
probe-resp	Configures probe response frame matching
reassoc	Configures re-association frame matching

Usage Guidelines

The frame type configured determines the SSID match type configured. To configure the SSID match type as SSID, the frame type must be beacon, probe-req or probe-resp.

Example

```
rfs6000-37FABE(config-test-signature-test)#frame-type reassoc

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Resets a WIPS signature frame type

20.1.7.2.5 interference-event

signature mode commands

Configures this WIPS policy signature as Smart RF interference source

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
interference-event
```

Parameters

None

Example

```
rfs6000-37FABE(config-test-signature-test)#interference-event

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Disables this WIPS policy signature as Smart RF interference source

20.1.7.2.6 mode

signature mode commands

Enables a WIPS policy signature

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mode enable
```

Parameters

- `mode enable`

mode enable	Enables this WIPS signature

Example

```
rfs6000-37FABE(config-test-signature-test)#mode enable
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Disables a WIPS signature

20.1.7.2.7 payload

signature mode commands

Configures payload settings. The payload command sets a numerical index pattern and offset for this WIPS signature.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
payload <1-3> pattern <WORD> offset <0-255>
```

Parameters

```
payload <1-3> pattern <WORD> offset <0-255>
```

payload <1-3>	Configures payload settings • <1-3> – Sets the payload index from 1 - 3.
pattern <WORD>	Specifies the pattern to match: hex or string • <WORD> – Sets the pattern name
offset <0-255>	Specifies the payload offset to start the pattern match • <0-255> – Sets the offset value from 0 - 255

Example

```
rfs6000-37FABE(config-test-signature-test)#payload 1 pattern test offset 1

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type assoc
  filter-ageout 8
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Removes payload and associated settings

20.1.7.2.8 src-mac

signature mode commands

Configures a source MAC address for a packet examined for matching

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
src-mac <MAC>
```

Parameters

- `src-mac <MAC>`

src-mac <MAC>	Configures the source MAC address to match • <MAC> – Specify the source MAC address.

Example

```
rfs6000-37FABE(config-test-signature-test)#src-mac 00-1E-E5-EA-1D-60

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type assoc
  filter-ageout 8
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Removes a WIPS signature source MAC address

20.1.7.2.9 ssid-match

signature mode commands

Configures the SSID (and its character length) used for matching

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ssid-match [ssid|ssid-len]

ssid-match [ssid <SSID>|ssid-len <0-32>]
```

Parameters

- `ssid-match [ssid <SSID>|ssid-len <0-32>]`

ssid <SSID>	Specifies the SSID match string • <SSID> – Specify the SSID string. **Note:** Specify the correct SSID to ensure proper filtering.
ssid-len <0-32>	Specifies the length of the SSID • <0-32> – Specify the SSID length from 0 - 32 characters.

Example

```
rfs6000-37FABE(config-test-signature-test)#ssid-match ssid PrinterLan

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Removes the configured SSID

20.1.7.2.10 threshold-client

signature mode commands

Configures the wireless client threshold limit. When the wireless client exceeds the specified limit, an event is triggered.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
threshold-client <1-65535>
```

Parameters

- `threshold-client <1-65535>`

threshold-client <1-65535>	Configures the wireless client threshold limit • <1-65535> – Sets the threshold limit for a 60 second window from 1 - 65535

Example

```
rfs6000-37FABE(config-test-signature-test)#threshold-client 88

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Removes the wireless client threshold limit configured with a WIPS policy signature

20.1.7.2.11 threshold-radio

signature mode commands

Configures the radio's threshold limit. When the radio exceeds the specified limit, an event is triggered.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
threshold-radio <1-65535>
```

Parameters

- `threshold-radio <1-65535>`

threshold-radio <1-65535>	Configures the radio's threshold limit • <1-65535> – Specify the threshold limit for a 60 second window from 1 - 65535.

Example

```
rfs6000-37FABE(config-test-signature-test)#threshold-radio 88

rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  threshold-radio 88
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)#
```

Related Commands

no	Removes the radio's threshold limit configured with a WIPS policy signature

20.1.7.2.12 no

signature mode commands

Negates a command or resets settings to their default. When used in the config WIPS policy signature mode, the `no` command resets or removes WIPS signature settings.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [bssid|dst-mac|filter-ageout|frame-type|interference-event|mode|payload|src-mac|ssid-match|threshold-client|threshold-radio]

no [bssid|dts-mac|filter-ageout|frame-type|interference-event|mode enable|payload <1-3>|src-mac|ssid-match [ssid|ssid-len]|threshold-client|threshold-radio]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or resets settings to their default

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following is the WIPS signature 'test' settings before the execution of the 'no' command:

```
rfs6000-37FABE(config-test-signature-test)#show context
 signature test
  bssid 11-22-33-44-55-66
  src-mac 00-1E-E5-EA-1D-60
  dst-mac 55-66-77-88-99-00
  frame-type beacon
  ssid-match ssid PrinterLan
  filter-ageout 8
  threshold-client 88
  threshold-radio 88
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)#
```

The following is the WIPS signature ‘test’ settings after the execution of the ‘no’ command:

```
rfs6000-37FABE(config-test-signature-test)#no mode enable
rfs6000-37FABE(config-test-signature-test)#no bssid
rfs6000-37FABE(config-test-signature-test)#no dst-mac
rfs6000-37FABE(config-test-signature-test)#no src-mac
rfs6000-37FABE(config-test-signature-test)#no filter-ageout
rfs6000-37FABE(config-test-signature-test)#no threshold-client
rfs6000-37FABE(config-test-signature-test)#no threshold-radio

rfs6000-37FABE(config-test-signature-test)#
 signature test
  no mode enable
  frame-type beacon
  payload 1 pattern test offset 1
rfs6000-37FABE(config-test-signature-test)
```

20.1.8 use

wips-policy

Enables device categorization on this WIPS policy. This command uses an existing device categorization list. The list categorizes devices as authorized or unauthorized.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use device-categorization <DEVICE-CATEGORIZATION>
```

Parameters

- `use device-categorization <DEVICE-CATEGORIZATION>`

device-categorization <DEVICE-CATEGORIZATION>	Configures a device categorization list • <DEVICE-CATEGORIZATION> – Specify the device categorization object name to associate with this profile

Example

```
rfs6000-37FABE(config-wips-policy-test)#use device-categorization test

rfs6000-37FABE(config-wips-policy-test)#show context
wips-policy test
 event excessive 80211-replay-check-failure threshold-client 10 threshold-radio 99
filter-ageout 9
 no event client-anomaly wellenreiter filter-ageout 99
 signature test
  interference-event
  bssid 11-22-33-44-55-66
  dst-mac 55-66-77-88-99-00
  frame-type reassoc
  filter-ageout 8
  threshold-client 88
  payload 1 pattern test offset 1
 ap-detection-ageout 50
 ap-detection-wait-time 15
 use device-categorization test
rfs6000-37FABE(config-wips-policy-test)#
```

Related Commands

no	Disables the use of a device categorization policy with a WIPS policy

21 WLAN-QOS-POLICY

This chapter summarizes the WLAN QoS policy in the CLI command structure.

A WLAN QoS policy increases network efficiency by prioritizing data traffic. Prioritization reduces congestion. This is essential because of the lack of bandwidth for all users and applications. QoS helps ensure each WLAN on the wireless controller receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as Video, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN

Each WLAN QoS policy has a set of parameters which it groups into categories, such as management, voice and data. Packets within each category are processed based on the weights defined for each WLAN.

Use the (config) instance to configure WLAN QoS policy commands. To navigate to the WLAN QoS policy instance, use the following commands:

```
<DEVICE>(config)#wlan-qos-policy <POLICY-NAME>

rfs6000-37FABE(config)#wlan-qos-policy test
rfs6000-37FABE(config-wlan-qos-test)#?
WLAN QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address and
                         forwarding QoS classification
  classification         Select how traffic on this WLAN must be classified
                         (relative prioritization on the radio)
  multicast-mask         Egress multicast mask (frames that match bypass the
                         PSPqueue. This permits intercom mode operation
                         without delay even in the presence of PSP clients)
  no                     Negate a command or set its defaults
  qos                    Quality of service
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-wlan/per-client basis
  svp-prioritization     Enable spectralink voice protocol support on this wlan
  voice-prioritization   Prioritize voice client over other client (for
                         non-WMM clients)
  wmm                    Configure 802.11e/Wireless MultiMedia parameters

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal
rfs6000-37FABE(config-wlan-qos-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

21.1 wlan-qos-policy

- *WLAN-QOS-POLICY*

WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients these access point radios support.

The following table summarizes WLAN QoS policy configuration commands:

Table 21.1 *WLAN-QoS-Policy-Config Commands*

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast stream addresses and forwards QoS classifications	*page 21-3*
classification	Classifies WLAN traffic based on priority	*page 21-5*
multicast-mask	Configures the egress prioritization multicast mask	*page 21-7*
no	Negates a command or sets its default	*page 21-8*
qos	Defines the QoS configuration	*page 21-9*
rate-limit	Configures the WLAN traffic rate limit using a WLAN QoS policy	*page 21-10*
svp-prioritization	Enables Spectralink voice protocol support on a WLAN	*page 21-13*
voice-prioritization	Prioritizes voice client over other clients	*page 21-14*
wmm	Configures 802.11e/wireless multimedia parameters	*page 21-15*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

21.1.1 accelerated-multicast

wlan-qos-policy

Configures the accelerated multicast stream address and forwarding QoS classification settings

Enabling this option allows the system to automatically detect and convert multicast streams to unicast streams. When a stream is converted and queued up for transmission, there are a number of classification mechanisms that can be applied to the stream. Use the classification options to specify the traffic type to prioritize.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
accelerated-multicast [<IP>|autodetect]

accelerated-multicast [<IP>|autodetect] {classification [background|best-effort|trust|video|voice]}
```

Parameters

- `accelerated-multicast [<IP>|autodetect] {classification [background|best-effort|trust|video|voice]}`

accelerated-multicast	Configures the accelerated multicast stream address and forwarding QoS classification
<IP>	Configures a multicast IP address in the A.B.C.D format. The system can configure up to 32 IP addresses for each WLAN QoS policy
autodetect	Allows the system to automatically detect multicast streams to be accelerated. This parameter allows the system to convert multicast streams to unicast, or to specify multicast streams converted to unicast.
classification	Optional. Configures the QoS classification (traffic class) settings. When the stream is converted and queued for transmission, specify the type of classification applied to the stream. The options are: background, best-effort, trust, voice, and video.
background	Forwards streams with background (low) priority. This parameter is common to both <IP> and auto detect.
best-effort	Forwards streams with best effort (normal) priority. This parameter is common to both <IP> and autodetect.
trust	No change to the streams forwarding traffic class. This parameter is common to both <IP> and autodetect.
video	Forwards streams with video traffic priority. This parameter is common to both <IP> and autodetect.
voice	Forwards streams with voice traffic priority. This parameter is common to both <IP> and autodetect.

Example

```
rfs6000-37FABE(config-wlan-qos-test)#accelerated-multicast autodetect
classification voice

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.2 classification

wlan-qos-policy

Specifies how traffic on this WLAN is classified. This classification is based on relative prioritization on the radio.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
classification [low|non-unicast|non-wmm|normal|video|voice|wmm]

classification [low|normal|video|voice|wmm]

classification non-unicast [voice|video|normal|low|default]

classification non-wmm [voice|video|normal|low]
```

Parameters

- `classification [low|normal|video|voice|wmm]`

low	Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio
normal	Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio
video	Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio
voice	Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio
wmm	Uses WMM based classification, using DSCP or 802.1p tags, to classify traffic into different queues Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the access point to be prioritized according to the type of traffic (voice, video etc). The WMM classification supports high throughput data rates required for 802.11n device support. This is the default setting.

- `classification non-unicast [voice|video|normal|low|default]`

non-unicast	Optimized for non-unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multiple destinations
video	Optimized for non-unicast video traffic. Implies all WLAN non-unicast traffic is classified and treated as video packets
voice	Optimized for non-unicast voice traffic. Implies all WLAN non-unicast traffic is classified and treated as voice packets
normal	Optimized for non-unicast best effort traffic. Implies all WLAN non-unicast traffic is classified and treated as normal priority packets (best effort).

low	Optimized for non-unicast background traffic. Implies all WLAN non-unicast traffic is classified and treated as low priority packets (background)
default	Uses the default classification mode (same as unicast classification if WMM is disabled, normal if unicast classification is WMM). This is the default setting.

- `classification non-wmm [voice|video|normal|low]`

non-wmm	Specifies how traffic from non-WMM clients is classified
voice	Optimized for non-WMM voice traffic. Implies all WLAN non-WMM client traffic is classified and treated as voice packets
video	Optimized for non-WMM video traffic. Implies all WLAN non-WMM client traffic is classified and treated as video packets
normal	Optimized for non-WMM best effort traffic. Implies all WLAN non-WMM client traffic is classified and treated as normal priority packets (best effort). This is the default setting.
low	Optimized for non-WMM background traffic. Implies all WLAN non-WMM client traffic is classified and treated as low priority packets (background)

Example

```
rfs6000-37FABE(config-wlan-qos-test)#classification wmm

rfs6000-37FABE(config-wlan-qos-test)#classification non-wmm video

rfs6000-37FABE(config-wlan-qos-test)#classification non-unicast normal

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.3 multicast-mask

wlan-qos-policy

Configures an egress prioritization multicast mask for this WLAN QoS policy

Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary or secondary prioritization multicast mask, the network administrator can indicate which packets are transmitted immediately.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
multicast-mask [primary|secondary] <MAC/MASK>
```

Parameters

- `multicast-mask [primary|secondary] <MAC/MASK>`

primary <MAC/MASK>	Configures the primary egress prioritization multicast mask • <MAC/MASK> – Provide the MAC address and the mask in the AA-BB-CC-DD-EE-FF /XX-XX-XX-XX-XX-XX-XX format. The default value is 00-00-00-00-00-00/FF-FF-FF-FF-FF-FF. **Note:** Setting masks is optional and only needed if there are traffic types requiring special handling.
secondary <MAC/ MASK>	Configures the secondary egress prioritization multicast mask • <MAC/MASK> – Provide the MAC address and the mask in the AA-BB-CC-DD-EE-FF /XX-XX-XX-XX-XX-XX-XX format. The default value is 00-00-00-00-00-00/FF-FF-FF-FF-FF-FF.

Example

```
rfs6000-37FABE(config-wlan-qos-test)#multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.4 no

wlan-qos-policy

Negates a command or resets settings to their default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [accelerated-multicast|classification|multicast-mask|qos|rate-limit|svp-
prioritization|voice-prioritization|wmm]

no [accelerated-multicast [<IP>|autodetect]|classification {non-unicast|non-wmm}|
multicast-mask [primary|secondary]|qos trust [dscp|wmm]|svp-prioritization|voice-
prioritization]

no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold}
no rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold
[background|best-effort|video|voice]}

no wmm [background|best-effort|power-save|qbss-load-element|video|voice]
no wmm [power-save|qbss-load-element]
no wmm [backgorund|best-effort|video|voice] [aifsn|cw-max|cw-min|txop-limit]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates a command or resets settings to their default

Example

The following example shows the WLAN QoS Policy ‘test’ settings before the ‘no’ commands are executed:

```
rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#

rfs6000-37FABE(config-wlan-qos-test)#no classification non-wmm
rfs6000-37FABE(config-wlan-qos-test)#no multicast-mask primary
rfs6000-37FABE(config-wlan-qos-test)#no qos trust dscp
```

The following example shows the WLAN QoS Policy ‘test’ settings after the ‘no’ commands are executed:

```
rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast normal
 no qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.5 qos

wlan-qos-policy

Enables QoS on this WLAN

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
qos trust [dscp|wmm]
```

Parameters

- `qos trust [dscp|wmm]`

trust [dscp|wmm]	Trusts the QoS values of ingressing packets. Both these options are enabled by default. • dscp – Trusts the IP DSCP values of ingressing packets • wmm – Trusts the 802.11 WMM QoS values of ingressing packets

Example

```
rfs6000-37FABE(config-wlan-qos-test)#qos trust wmm
rfs6000-37FABE(config-wlan-qos-test)#qos trust dscp

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-unicast normal
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.6 rate-limit

wlan-qos-policy

Configures the WLAN traffic rate limits using the WLAN QoS policy

Excessive traffic causes performance issues or brings down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, settings defined on the controller (access point, wireless controller, or service platform) are applied. An administrator can set separate QoS rate limits for upstream (data transmitted from the managed network) and downstream (data transmitted to the managed network).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, it is recommended that you define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) are dropped resulting in intermittent outages and performance problems.

Connected wireless clients can also have QoS rate limit settings defined in both the upstream and downstream direction.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
rate-limit [client|wlan] [from-air|to-air] {max-burst-size|rate|red-threshold}

rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000>}

rate-limit [client|wlan] [from-air|to-air] {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}
```

Parameters

```
• rate-limit [client|wlan] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000>}
```

rate-limit	Configures traffic rate limit parameters
client	Configures traffic rate limiting parameters on a per-client basis
wlan	Configures traffic rate limiting parameters on a per-WLAN basis
from-air	Configures traffic rate limiting from a wireless client to the network
to-air	Configures the traffic rate limit from the network to a wireless client

max-burst-size <2-1024>	Optional. Sets the maximum burst size from 2 - 1024 kbytes. The chances of the upstream or downstream packet transmission getting congested for the WLAN's client destination are reduced for smaller burst sizes. The default values are: - WLAN 'to-air' and 'from-air': 320 kbytes - Client 'to-air' and 'from-air': 64 kbytes
	Smaller the burst, lesser are the chances of upstream packet transmission resulting in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site.
rate <50-1000000>	Optional. Sets the traffic rate from 50 - 1000000 Kbps. This limit is the threshold value for the maximum number of packets received or transmitted over the WLAN from all access categories. Any traffic that exceeds the specified rate is dropped and a log message is generated. The default values are: - WLAN 'to-air' and 'from-air': 5000 kbytes - Client 'to-air' and 'from-air': 1000 kbytes

- `rate-limit [client|wlan] [from-air|to-air] {red-threshold [background <0-100>| best-effort <0-100>|video <0-100>|voice <0-100>]}`

rate-limit	Configures traffic rate limit parameters
client	Configures traffic rate limiting parameters on a per-client basis
wlan	Configures traffic rate limiting parameters on a per-WLAN basis
from-air	Configures traffic rate limiting from a wireless client to the network
to-air	Configures the traffic rate limit from the network to a wireless client
red-threshold	Configures random early detection threshold values for a designated traffic class
background <0-100>	Optional. Sets the maximum burst size from 2 - 1024 kbytes. The chances of the upstream or downstream packet transmission getting congested for the WLAN's client destination are reduced for smaller burst sizes. The default values are: - WLAN 'to-air' and 'from-air': 320 kbytes - Client 'to-air' and 'from-air': 64 kbytes Smaller the burst, lesser are the chances of upstream packet transmission resulting in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site.
best-effort <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for best effort traffic in the upstream or downstream direction. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold values are: - WLAN 'to-air' and 'from-air': 50% - Client 'to-air' and 'from-air': 50%

video <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for video traffic in the upstream or downstream direction. Video traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold values are: - WLAN 'to-air' and 'from-air': 25% - Client 'to-air' and 'from-air': 25%
voice <0-100>	The following is common to the 'from-air' and 'to-air' parameters: Optional. Sets a percentage value for voice traffic in the upstream or downstream direction. Voice traffic exceeding the defined threshold is dropped and a log message is generated. The default threshold values are:. - WLAN 'to-air' and 'from-air': 0% - Client 'to-air' and 'from-air': 0% **Note:** A value of 0% means no early random drops.

Usage Guidelines

The following information should be taken into account when configuring rate limits:

- Background traffic consumes the least bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis).
- Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).
- Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).

Example

```
rfs6000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air max-burst-size 6

rfs6000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air rate 55

rfs6000-37FABE(config-wlan-qos-test)#rate-limit wlan from-air red-threshold best-
effort 10
rfs6000-37FABE(config-wlan-qos-test)#rate-limit client from-air red-threshold
background 3

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.7 svp-prioritization

wlan-qos-policy

Enables WLAN SVP support on this WLAN QoS policy. SVP support enables the identification and prioritization of traffic from Spectralink/Ploycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy VOIP phones. If the wireless client classification is WMM, non-WMM devices recognized as voice devices have all their traffic transmitted at voice priority. Devices are classified as voice, when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM.

This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
svp-prioritization
```

Parameters

None

Example

```
rfs6000-37FABE(config-wlan-qos-test)#svp-prioritization

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.8 voice-prioritization

wlan-qos-policy

Prioritizes voice clients over other clients (for non-WMM clients). This gives priority to voice and voice management packets and is supported only on certain legacy VOIP phones. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
voice-prioritization
```

Parameters

None

Example

```
rfs6000-37FABE(config-wlan-qos-test)#voice-prioritization

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization
 voice-prioritization
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

21.1.9 wmm

wlan-qos-policy

Configures 802.11e/*Wireless Multimedia* (WMM) parameters for this WLAN QoS policy

WMM makes it possible for both home networks and Enterprises to decide which data streams are most important and assign them a higher traffic priority.

WMM's prioritization capabilities are based on the four access categories (background, best-effort, video, and voice). Higher the *Access Category* (AC) higher is the transmission probability over the controller managed WLAN. ACs correspond to the 802.1d priorities, facilitating interoperability with QoS policy management mechanisms. WMM enabled controllers coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized as best effort by default. Applications assign each data packet to a given access category. Categorized packets are added to one of four independent transmit queues (one per access category). The client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client should be granted the *Opportunity to Transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category. These parameters are:

- The minimum interframe space, or *Arbitrary Inter-Frame Space Number* (AIFSN)
- The contention window, sometimes referred to as the random back off wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest back off values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest back off value gets the TXOP.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
wmm [background|best-effort|power-save|qbss-load-element|video|voice]

wmm [power-save|qbss-load-element]

wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```

Parameters

- `wmm [power-save|qbss-load-element]`

wmm	Configures 802.11e/wireless multimedia parameters

power-save	Enables support for the WMM-Powersave mechanism. This mechanism, also known as *Unscheduled Automatic Power Save Delivery* (U-APSD), is specifically designed for WMM voice devices. This feature is enabled by default.
qbss-load-element	Enables support for the *QOS Basic Service Set* (QBSS) load information element in beacons and probe response packets advertised by access packets. This feature is enabled by default.

- `wmm [background|best-effort|video|voice] [aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]`

wmm	Configures 802.11e/wireless multimedia parameters. This parameter enables the configuration of four access categories. Applications assign each data packet to one of these four access categories and queues them for transmission.
background	Configures background access category parameters
best-effort	Configures best effort access category parameters. Packets not assigned to any particular access category are categorized by default as having best effort priority
video	Configures video access category parameters
voice	Configures voice access category parameters
aifsn <2-15>	Configures *Arbitrary Inter-Frame Space Number* (AIFSN) from 2 - 15. AIFSN is the wait time between data frames. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 2 The default for traffic best effort (normal) categories is 3 The default for traffic background (low) categories is 7 • <2-15> – Sets a value from 2 - 15
cw-max <0-15>	Configures the maximum contention window. Wireless clients pick a number between 0 and the minimum contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 3 The default for traffic video categories is 4 The default for traffic best effort (normal) categories 10 The default for traffic background (low) categories is 10 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15.

cw-min <0-15>	Configures the minimum contention window. Wireless clients pick a number between 0 and the min contention window to wait before retransmission. Wireless clients then double their wait time on a collision, until it reaches the maximum contention window. This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 2 The default for traffic video categories is 3 The default for traffic best effort (normal) categories is 4 The default for traffic background (low) categories is 4 • <0-15> – ECW: the contention window. The actual value used is (2^ECW - 1). Set a value from 0 - 15.
txop-limit <0-65535>	Configures the transmit-opportunity (the interval of time during which a particular client has the right to initiate transmissions). This parameter is common to background, best effort, video and voice. The default for traffic voice categories is 47 The default for traffic video categories is 94 The default for traffic best effort (normal) categories is 0 The default for traffic background (low) categories is 0 • <0-65535> – Set a value from 0 - 65535 to configure the transmit-opportunity in 32 microsecond units.

Example

```
rfs6000-37FABE(config-wlan-qos-test)#wmm video txop-limit 9
rfs6000-37FABE(config-wlan-qos-test)#wmm voice cw-min 6

rfs6000-37FABE(config-wlan-qos-test)#show context
wlan-qos-policy test
 classification non-wmm video
 svp-prioritization
 voice-prioritization
 wmm video txop-limit 9
 wmm voice cw-min 6
 multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
 classification non-unicast normal
 rate-limit wlan from-air rate 55
 rate-limit wlan from-air max-burst-size 6
 rate-limit wlan from-air red-threshold best-effort 10
 rate-limit client from-air red-threshold background 3
 qos trust dscp
 qos trust wmm
 accelerated-multicast autodetect classification voice
rfs6000-37FABE(config-wlan-qos-test)#
```

22 L2TPV3-POLICY

This chapter summarizes *Layer 2 Tunnel Protocol Version 3* (L2TPv3) policy commands in the CLI command structure.

L2TPv3 is an IETF standard used for transporting different types of layer 2 frames over an intermediate IP network. L2TPv3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes. Use L2TPv3 to create tunnels for transporting layer 2 frames. L2TPv3 enables WING supported controllers and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TPv3 tunnels can be defined between WING devices and other vendor devices supporting the L2TPv3 protocol.

Multiple pseudowires can be created within an L2TPv3 tunnel. WING supported devices support an Ethernet VLAN pseudowire type exclusively. A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network. Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (an L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

NOTE: A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TPv3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TPv3 sessions. Each tunnel session corresponds to one pseudowire. An L2TPv3 control connection (a L2TPv3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TPv3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TPv3 session establishment. An L2TPv3 session created within an L2TPv3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If a L2TPv3 session is down, the pseudowire associated with it must be shut down. The L2TPv3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

NOTE: If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

This chapter is organized into the following sections:

- *l2tpv3-policy-commands*
- *l2tpv3-tunnel-commands*
- *l2tpv3-manual-session-commands*

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

22.1 l2tpv3-policy-commands

L2TPV3-POLICY

Use the (config) instance to configure L2TPv3 policy parameters. To navigate to the L2TPv3 policy instance, use the following commands:

```
<DEVICE>(config)#l2tpv3 policy <L2TPV3-POLICY-NAME>

rfs6000-37FABE(config)#l2tpv3 policy L2TPV3Policy1
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#?
L2tpv3 Policy Mode commands:
  cookie-size             Size of the cookie field present in each l2tpv3 data
                          message
  failover-delay          Time interval for re-establishing the tunnel after
                          the failover (RF-Domain
                          manager/VRRP-master/Cluster-master failover)
  force-l2-path-recovery  Enables force learning of servers, gateways etc.,
                          behind the l2tpv3 tunnel when the tunnel is
                          established
  hello-interval          Configure the time interval (in seconds) between
                          l2tpv3 Hello keep-alive messages exchanged in l2tpv3
                          control connection
  no                      Negate a command or set its defaults
  reconnect-attempts      Maximum number of attempts to reestablish the
                          tunnel.
  reconnect-interval      Time interval between the successive attempts to
                          reestablish the l2tpv3 tunnel
  retry-attempts          Configure the maximum number of retransmissions for
                          signaling message
  retry-interval          Time interval (in seconds) before the initiating a
                          retransmission of any l2tpv3 signaling message
  rx-window-size          Number of signaling messages that can be received
                          without sending the acknowledgment
  tx-window-size          Number of signaling messages that can be sent
                          without receiving the acknowledgment

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

The following table summarizes L2TPv3 policy configuration commands:

Table 22.1 *L2TPV3-Tunnel-Policy-Config Commands*

Command	Description	Reference
cookie-size	Configures the cookie field size for each L2TPv3 data packet	*page 22-5*
failover-delay	Configures the L2TPv3 tunnel failover delay in seconds	*page 22-6*
force-l2-path-recovery	Enables the forced detection of servers and gateways behind the L2TPv3 tunnel	*page 22-7*
hello-interval	Configures the interval, in seconds, between L2TPv3 “Hello” keep-alive messages exchanged in the L2TPv3 control connection	*page 22-8*

Table 22.1 *L2TPV3-Tunnel-Policy-Config Commands*

Command	Description	Reference
no	Negates or reverts L2TPv3 tunnel commands	*page 22-9*
reconnect-attempts	Configures the maximum number of retransmissions for signalling messages	*page 22-10*
reconnect-interval	Configures the interval, in seconds, between successive attempts to re-establish a failed tunnel connection	*page 22-11*
retry-attempts	Configures the maximum number of retransmissions of signalling messages	*page 22-12*
retry-interval	Configures the interval, in seconds, before initiating a retransmission of any L2TPv3 signalling message	*page 22-13*
rx-window-size	Configures the number of signalling messages received without sending an acknowledgment	*page 22-14*
tx-window-size	Configures the number of signalling messages transmitted without receiving an acknowledgment	*page 22-15*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

22.1.1 cookie-size

l2tpv3-policy-commands

Configures the size of the cookie field present in each L2TPv3 data packet. L2TPv3 data packets contain a session cookie that identifies the session (pseudowire) corresponding to it. In a tunnel, the cookie is a 4-byte or 8-byte signature shared between the two tunnel endpoints. This signature is configured at both the source and destination routers. If the signature at both ends do not match, the data is dropped. All sessions within a tunnel have the same session cookie size.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
cookie-size [0|4|8]
```

Parameters

- `cookie-size [0|4|8]`

cookie-size [0|4|8]	Configures the cookie-field size for each data packet. Select one of the following options: • 0 – No cookie field present in each L2TPv3 data message (this is the default setting) • 4 – 4 byte cookie field present in each L2TPv3 data message • 8 – 8 byte cookie field present in each L2TPv3 data message

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#cookie-size 8

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 cookie-size 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the cookie-field size to its default (0 - no cookie field present in each L2TPv3 data packet)

22.1.2 failover-delay

l2tpv3-policy-commands

Configures the L2TPv3 tunnel failover delay in seconds. This is the interval after which a failed over tunnel is re-established.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
failover-delay <5-60>
```

Parameters

- `failover-delay <5-60>`

failover-delay <5-60>	Sets the delay interval to re-establish a failed L2TPv3 tunnel (RF-Domain manager/ VRRP-master/Cluster-master failover) • <5-60> – Specify a failover delay from 5 - 60 seconds. The default is 5 seconds.

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#failover-delay 30

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 failover-delay 30
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the failover interval to its default (5 seconds)

22.1.3 force-l2-path-recovery

l2tpv3-policy-commands

Enables the forced detection of servers and gateways behind the L2TPv3 tunnel. This feature is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
force-l2-path-recovery
```

Parameters

None

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#force-l2-path-recovery

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 failover-delay 30
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
 force-l2-path-recovery
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Disables the forced detection of servers and gateways behind the L2TPv3 tunnel

22.1.4 hello-interval

l2tpv3-policy-commands

Configures the interval, in seconds, between L2TPv3 “Hello” keep-alive messages exchanged in a L2TPv3 control connection.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
hello-interval <1-3600>
```

Parameters

- `hello-interval <1-3600>`

hello-interval <1-3600>	Configures the interval for L2TPv3 “Hello” keep-alive messages • <1-3600> – Specify a value from 1 - 3600 seconds (default is 60 seconds).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#hello-interval 200

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the “Hello” keep-alive message interval to its default of 60 seconds

22.1.5 no

l2tpv3-policy-commands

Negates or reverts L2TPv3 policy settings to default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [cookie-size|failover-delay|force-l2-path-recovery|hello-interval|reconnect-attempts|reconnect-interval|retry-attempts|retry-interval|rx-window-size|tx-window-size]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates or reverts L2TPv3 policy settings to default

Example

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 50
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no hello-interval
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-attempts
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no reconnect-interval
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no retry-attempts
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no retry-interval
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#no cookie-size
```

The following example shows the l2tpv3 policy 'L2TPV3Policy1' settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

22.1.6 reconnect-attempts

l2tpv3-policy-commands

Configures the maximum number of attempts made to re-establish a tunnel connection

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
reconnect-attempts <0-8>
```

Parameters

- `reconnect-attempts <0-8>`

reconnect-attempts <0-8>	Configures the maximum number of attempts made to re-establish a tunnel connection • <0-8> – Specify a value from 0 - 8 (default is 0: configures infinite reconnect attempts).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-attempts 8

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the maximum number of reconnect attempts to default (0: configures infinite reconnect attempts)

22.1.7 reconnect-interval

l2tpv3-policy-commands

Configures the interval, in seconds, between two successive attempts to re-establish a failed tunnel connection

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
reconnect-interval <1-3600>
```

Parameters

- `reconnect-interval <1-3600>`

reconnect-interval <1-3600>	Configures the interval between successive attempts to re-establish a failed tunnel connection • <1-3600> – Specify a value from 1 - 3600 seconds (default is 120 seconds).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#reconnect-interval 100

l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the interval between successive attempts to re-establish a failed tunnel connection to default (120 seconds)

22.1.8 retry-attempts

l2tpv3-policy-commands

Configures the maximum number of attempts made to retransmit signalling messages. Use this command to specify how many retransmission cycles occur before determining the target tunnel peer is not reachable.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
retry-attempts <1-10>
```

Parameters

- `retry-attempts <1-10>`

retry-attempts <1-10>	Configures the maximum number of attempts made to retransmit signalling messages • <1-10> – Specify a value from 1 - 10 (default is 5 attempts).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#retry-attempts 10

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the maximum number of retransmissions of signalling messages to default (5 attempts)

22.1.9 retry-interval

l2tpv3-policy-commands

Configures the interval, in seconds, between two successive attempts at retransmitting a L2TPv3 signalling message

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
retry-interval <1-250>
```

Parameters

- `retry-interval <1-250>`

retry-interval <1-250>	Configures the interval, in seconds, between two successive retransmission attempts • <1-250> – Specify a value from 1 - 250 seconds (default is 5 seconds).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#retry-interval 30

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 reconnect-interval 100
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the retry interval to default (5 seconds)

22.1.10 rx-window-size

l2tpv3-policy-commands

Configures the number of signalling packets received without sending an acknowledgment

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
rx-window-size <1-15>
```

Parameters

- `rx-window-size <1-15>`

rx-window-size <1-15>	Configures the number of packets received without sending an acknowledgment • <1-15> – Specify a value from 1 - 15 (default is 10 packets).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#rx-window-size 9

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the number of packets received without sending an acknowledgment to default (10 packets)

22.1.11 tx-window-size

l2tpv3-policy-commands

Configures the number of signalling packets transmitted without receiving an acknowledgment

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
tx-window-size <1-15>
```

Parameters

- `tx-window-size <1-15>`

tx-window-size <1-15>	Configures the number of packets transmitted without receiving an acknowledgment • <1-15> – Specify a value from 1 - 15 (default is 10 packets).

Example

```
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#tx-window-size 9

rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#show context
l2tpv3 policy L2TPV3Policy1
 hello-interval 200
 retry-attempts 10
 retry-interval 30
 cookie-size 8
 rx-window-size 9
 tx-window-size 9
 reconnect-interval 100
 reconnect-attempts 8
rfs6000-37FABE(config-l2tpv3-policy-L2TPV3Policy1)#
```

Related Commands

no	Resets the number of packets transmitted without receiving an acknowledgment to default (10 packets)

22.2 l2tpv3-tunnel-commands

L2TPV3-POLICY

Use the (profile or device context) instance to configure a L2TPv3 tunnel. To navigate to the tunnel configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 tunnel <TUNNEL-NAME>

rfs6000-37FABE(config-profile-default-rfs7000)#l2tpv3 tunnel Tunnel1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#?
L2tpv3 Tunnel Mode commands:
  establishment-criteria  Set tunnel establishment criteria
  fast-failover           Configure fast failover for l2tpv3 tunnels
  hostname                Tunnel specific local hostname
  local-ip-address        Configure the IP address for tunnel. If not
                          specified, tunnel source ip address would be chosen
                          automatically based on the tunnel peer ip address
  mtu                     Configure the mtu size for the tunnel
  no                      Negate a command or set its defaults
  peer                    Configure the l2tpv3 tunnel peers. At least one peer
                          must be specified
  router-id               Tunnel specific local router ID
  session                 Create / modify the specified l2tpv3 session
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

The following table summarizes L2TPv3 tunnel configuration commands:

Table 22.2 *L2TPV3-Tunnel-Config Commands*

Command	Description	Reference
establishment-criteria	Configures L2TPv3 tunnel establishment criteria	*page 22-17*
fast-failover	Configures fast-failover support on the L2TPv3 tunnel	*page 22-19*
hostname	Configures tunnel specific local hostname	*page 22-20*
local-ip-address	Configures the tunnel's IP address	*page 22-21*
mtu	Configures the tunnel's *Maximum Transmission Unit* (MTU) size	*page 22-22*
no	Negates or reverts L2TPv3 tunnel commands	*page 22-23*
peer	Configures the tunnel's peers	*page 22-24*
router-id	Configures the tunnel's local router ID	*page 22-28*
session	Creates/modifies specified L2TPv3 session	*page 22-29*
use	Configures a tunnel to use a specified L2TPv3 tunnel policy	*page 22-31*

22.2.1 establishment-criteria

l2tpv3-tunnel-commands

Configures L2TPv3 tunnel establishment criteria

A L2TPv3 tunnel is established from the current device to the NOC controller when the current device becomes the VRRP master, cluster master, or RF Domain manager. Similarly, the L2TPv3 tunnel is closed when the current device switches to standby or backup mode.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

Parameters

```
• establishment-criteria [always|cluster-master|rf-domain-manager|vrrp-master <1-255>]
```

always	Always establishes a L2TPv3 tunnel from the current device to the NOC controller. This is the default setting. The 'always' option indicates the device need not be a cluster-master, rf-domain-manager, or vrrp-master to establish a tunnel.
cluster-master	Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the cluster master **Note:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.
rf-domain-manager	Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the RF Domain manager **Note:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.
vrrp-master <1-255>	Establishes a L2TPv3 tunnel from the current device to the NOC controller, only when the current device becomes the VRRP master • <1-255> – Specify the VRRP group number from 1 - 255. **Note:** The L2TPv3 tunnel is closed when the current device switches back the standby or backup mode.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-
Tunnel1)#establishment-criteria cluster-master

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Resets to default (always)

22.2.2 fast-failover

l2tpv3-tunnel-commands

Configures fast-failover support on the L2TPv3 tunnel. When configured, devices, using this profile, send tunnel requests to both peers, and in turn, establish tunnels with both peers. If not configured, tunnel establishment occurs on one peer, with failover and other functionality the same as legacy behavior. In case fast failover is configured when an active tunnel, with one peer, already exists, the tunnel establishment process is re-initiated with both peers. Of the two tunnels established, one is marked active while the other is standby. The sessions and routes from the active tunnel are only pushed to the dataplane, resulting in creation of data sessions. However, if the active tunnel fails, sessions and routes from the standby tunnel are pushed to the dataplane thereby providing almost immediate fail over. Both tunnels individually perform connection health checkups through hello intervals. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
fast-failover {aggressive}
```

Parameters

- `fast-failover {aggressive}`

fast-failover	Configures fast-failover support on the L2TPv3 tunnel
aggressive	Optional. When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of the number of retry attempts configured. This option is disabled by default. **Note:** The *hello-interval* and *retry-attempts* parameters are defined in the L2TPv3 Policy context. For more information on configuring an L2TPv3 policy, see *l2tpv3-policy-commands*. For more information on associating an L2TPv3 policy to an L2TPv3 tunnel, see *use*.

Example

```
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#show context
include-factory | include fast-failover
  no fast-failover
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#

nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#fast-failover
 aggressive

nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#show context
 l2tpv3 tunnel TestTunnel2
  fast-failover aggressive
nx9500-6C8809(config-profile testNX9500-l2tpv3-tunnel-TestTunnel2)#
```

Related Commands

no	Removes fast-failover support on the L2TPv3 tunnel

22.2.3 hostname

l2tpv3-tunnel-commands

Configures the tunnel's local hostname

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
hostname <WORD>
```

Parameters

- `hostname <WORD>`

hostname <WORD>	Configures the tunnel's local hostname • <WORD> – Specify the tunnel's local hostname.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#hostname
TunnelHost1

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  hostname TunnelHost1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Removes the tunnel's local hostname

22.2.4 local-ip-address

l2tpv3-tunnel-commands

Configures the tunnel's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel's peer IP address.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
local-ip-address <IP>
```

Parameters

- `local-ip-address <IP>`

local-ip-address <IP>	Configures the L2TPv3 tunnel's source IP address • <IP> – Specify the tunnel's IP address. Ensure the IP address is available (or will become available - virtual IP) on an interface. Modifying a tunnel's local IP address re-establishes the tunnel.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#local-ip-
address 172.16.10.2

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  hostname TunnelHost1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Resets the tunnel's local IP address and re-establishes the tunnel

22.2.5 mtu

l2tpv3-tunnel-commands

Configures the MTU size for this tunnel. This value determines the packet size transmitted over this tunnel.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mtu <128-1460>
```

Parameters

- `mtu <128-1460>`

mtu <128-1460>	Configures the MTU size for this tunnel • <128-1460> – Specify a value from 128 - 1460 bytes (default is 1460 bytes).

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#mtu 1280

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  mtu 1280
  hostname TunnelHost1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Resets the MTU size for this tunnel to default (1460 bytes)

22.2.6 no

l2tpv3-tunnel-commands

Negates or reverts a L2TPv3 tunnel settings to default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [establishment-criteria|fast-failover|hostname|local-ip-address|mtu|peer <1-2>|router-id|session|use]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates or reverts a L2TPv3 tunnel settings to default

Example

The tunnel settings before the 'no' command is executed:

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  local-ip-address 172.16.10.2
  mtu 1280
  hostname TunnelHost1
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

The tunnel settings after the 'no' command is executed:

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no local-ip
-address
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no mtu
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#no hostname

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

22.2.7 peer

l2tpv3-tunnel-commands

Configures the L2TPv3 tunnel's peers. At least one peer must be specified.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
peer <1-2> {hostname|ip-address|ipsec-secure|router-id|udp}

peer <1-2> {hostname [<HOSTNAME>|any]} {ipsec-secure|router-id|udp}
peer <1-2> {ip-address <IP>} {hostname|ipsec-secure|router-id|udp}
peer <1-2> {ipsec-secure} {gw [<IP>|<WORD>]}
peer <1-2> {router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}
peer <1-2> {udp} {ipsec-secure|port <1-65535>}
```

Parameters

- `peer <1-2> {hostname [<HOSTNAME>|any]} {ipsec-secure|router-id|udp}`

peer <1-2>	Configures the tunnel's peer ID • <1-2> – Specify the ID from 1 - 2. The peer ID identifies the primary (ID 1) secondary (ID 2) peers. The L2TPv3 tunnel is established with the primary peer. The secondary peer is used for tunnel failover. If the peer is not specified, tunnel establishment does not occur. **Note:** At any time the tunnel is established with only one peer, unless fast-failover support is configured on the L2TPv3 tunnel. For more information, see *fast-failover*.
hostname [<HOSTNAME>|any]	Optional. Configures the peers' hostname. The hostname options are: • <HOSTNAME> – Specifies the hostname as *Fully Qualified Domain Name* (FQDN) or partial DN or any other name • any – Peer name is not specified. If the hostname is 'any' this tunnel is considered as responder only and will allow incoming connection from any host.

ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer hostname, optionally specify the IPSec settings:
	• ipsec-secure – Optional. Enables auto IPSec on the L2TPv3 tunnel
	  • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway:
	  • <IP> – Configures IPSec gateway's IP address
	  • <WORD> – Configures IPSec gateway's hostname

router-id [<IP>|<WORD>|any]	After specifying the peer hostname, optionally specify router ID settings:
	• router-id – Optional. Configures the peer's router ID in one of the following formats:
	  • <IP> – Peer router ID in the IP address (A.B.C.D) format
	  • <WORD> – Peer router ID range (for example, 100-120)
	  • any – Peer router ID is not specified. This allows incoming connection from any router ID.

udp {ipsec-secure gw|port <1-65535> {ipsec-secure}}	After specifying the peer hostname, optionally specify UDP settings: The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> {ipsec-secure} – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

- `peer <1-2> {ip-address <IP>} {hostname|ipsec-secure|router-id|udp}`

peer <1-2>	Configures the tunnel's peer ID from 1 - 2. At any time the tunnel is established with only one peer.
ip-address <IP>	Optional. Configures the peer's IP address in the A.B.C.D format • <IP> – Specify the peer's IP address.
hostname [<FQDN>|any]	After specifying the peer IP address, optionally specify the peer's hostname: • hostname – Optional. Configures the peers' hostname. The hostname options are: • <FQDN> – Specifies the hostname as FQDN or partial DN • any – Peer name is not specified. If the hostname is 'any' this tunnel is considered as responder only and will allow incoming connection from any host.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer IP address, optionally specify the IPSec settings: • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname
router-id [<A.B.C.D>|<WORD>|any]	After specifying the peer IP address, optionally specify the router ID using one of the following options: • router-id – Optional. Configures the peer's router-id in one of the following formats: • <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format • <WORD> – Peer router ID range (for example, 100-120) • any – Peer router ID is not specified. This allows incoming connection from any router ID.
udp {ipsec-secure gw|port <1-65535> {ipsec-secure}}	After specifying the peer IP address, optionally specify the peer's UDP port settings: The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

- `peer <1-2> {ipsec-secure} {gw [<IP>|<WORD>]}`

peer <1-2>	Configures the tunnel's peer ID from 1 - 2. At any time the tunnel is established with only one peer.

ipsec-secure {gw [<IP>|<WORD>]}	Optional. Enables auto IPSec for this peer • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname

- `peer <1-2> {router-id [<IP>|<WORD>|any]} {ipsec-secure|udp}`

peer <1-2>	Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.
router-id [<A.B.C.D>|<WORD>| any]	Optional. Configures the peer's router-id in one of the following formats: • <A.B.C.D> – Peer router ID in the IP address (A.B.C.D) format • <WORD> – Peer router ID range (for example, 100-120) • any – Peer router ID is not specified. This allows incoming connection from any router ID.
ipsec-secure {gw [<IP>|<WORD>]}	After specifying the peer's router ID, optionally specify the IPSec settings. • ipsec-secure – Optional. Enables auto IPSec • gw – Optional. Configures the IPSec gateway. Use one of the following options to configure the IPSec gateway: • <IP> – Configures IPSec gateway's IP address • <WORD> – Configures IPSec gateway's hostname
udp {ipsec-secure gw| port <1-65535> {ipsec-secure}}	After specifying the peer's router ID, optionally specify the IPSec settings. The UDP option configures the encapsulation mode for this tunnel. • UDP – Optional. Configures UDP encapsulation (default encapsulation is IP) • ipsec-secure gw – Optional. Enables auto IPSec • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

- `peer <1-2> {udp} {ipsec-secure|port <1-65535>}`

peer <1-2>	Configures the tunnel peer ID from 1 - 2. At any time the tunnel is established with only one peer.
udp {ipsec-secure| port <1-65535> {ipsec-secure}}	Optional. Configures UDP encapsulation for this tunnel's pee (default encapsulation is IP) • ipsec-secure – Optional. Configures IPSec gateway on this peer UDP port • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service from 1 - 65535. After specifying the peer UDP port, optionally configure the IPSec settings.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#peer 2
hostname tunnel1peer1 udp port 100

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Removes the peer configured for this tunnel

22.2.8 router-id

l2tpv3-tunnel-commands

Configures the tunnel's local router ID

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
router-id [<1-4294967295>|<IP>]
```

Parameters

- `router-id [<1-4294967295>|<IP>]`

router-id [<1-4294967295>|<IP>]	Configures the tunnel's local router ID in one of the following formats: • <1-4294967295> – Router ID in the number format (from1 - 4294967295) • <IP> – Router ID in IP address format (A.B.C.D)

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#router-id
2000

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  router-id 2000
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Removes the tunnel's router ID

22.2.9 session

l2tpv3-tunnel-commands

Configures a session's pseudowire ID, which describes the session's purpose. The session established message sends this pseudowire ID to the L2TPv3 peer.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
session <L2TPV3-SESSION-NAME> [pseudowire-id|rate-limit]

session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source
   vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
session <L2TPV3-SESSION-NAME> rate-limit [egress|ingress] rate <50-1000000>
   max-burst-size <2-1024>
```

Parameters

- `session <L2TPV3-SESSION-NAME> pseudowire-id <1-4294967295> traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}`

session <L2TPV3-SESSION-NAME>	Configures this session's name • <L2TPV3-SESSION-NAME> – Specify the L2TPV3 session name (should not exceed 31 characters in length). A tunnel is usable only if it has one or more session(s) (having specific session names) configured. The L2TPv3 tunnel has no idle timeout, it closes when the last tunnel session is closed.
pseudowire-id <1-4294967295>	Configures the pseudowire ID for this session from 1- 4204067295 A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire is needed to encapsulate and tunnel layer 2 protocols across a layer 3 network.
traffic-source vlan <VLAN-ID-RANGE>	Configures VLAN as the traffic source for this tunnel • <VLAN-ID-RANGE> – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35).
native-vlan <1-4094>	Optional – Configures the native VLAN ID for this session, which is not tagged • <1-4094> – Specify the native VLAN ID from 1- 4094.

- `session <L2TPV3-SESSION-NAME> rate-limit [egress|ingress] rate <50-1000000> max-burst-size <2-1024>`

session <L2TPV3-SESSION-NAME>	Configures this session's name • <L2TPV3-SESSION-NAME> – Specify the L2TPV3 session name (should not exceed 31 characters in length). A tunnel is usable only if it has one or more session(s) (having specific session names) configured. The L2TPv3 tunnel has no idle timeout, it closes when the last tunnel session is closed.

rate-limit [egress|ingress]	Configures a rate for incoming and/or outgoing traffic on this L2TPv3 tunnel. When configured, this option limits the rate at which data is sent to or received from L2TPv3 tunnel members. • egress – Applies the specified rate to outbound traffic, from the L2TPv3 tunnel (going out from access points, wireless controllers, and service platforms) to the network • ingress – Applies the specified rate to inbound traffic, from the network to the L2TPV3 tunnel (coming in to access points, wireless controllers, and service platforms)
rate <50-1000000>	Specify the data rate, in kilobits per second, for the incoming and/or outgoing traffic • <50-1000000> – Specify a value from 50 - 1000000 kbps. The default is 5000 Kbps.
max-burst-size <2-1024>	Configures the maximum burst size, in kilobytes, for incoming/outgoing traffic rate limiting (depending on the direction selected) on a L2TPv3 tunnel. • <2-1024> – Specify the maximum burst size from 2 - 1024 kbytes. Smaller the burst size, lesser are the chances of the upstream packet transmission resulting in congestion of the L2TPv3 tunnel traffic. The default setting is 320 kbytes.

Usage Guidelines

The working status of a pseudowire is reflected by the state of the L2TPv3 session. If the corresponding session is L2TPv3 down, the pseudowire associated with it must be shut down.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#session
tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-vlan 1

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
 session tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-
vlan 1
  router-id 2000
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Removes a session

22.2.10 use

l2tpv3-tunnel-commands

Configures a tunnel to use a specified L2TPv3 tunnel policy and specified critical resources

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [critical-resource|l2tpv3-policy]
use critical-resource <CRM-NAME1> {<CRM-NAME2>} <CRM-NAME3>} <CRM-NAME4>}
use l2tpv3-policy <L2TPV3-POLICY-NAME>
```

Parameters

- `use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}`

use critical-resource <CRM-NAME1> {<CRM-NAME2>} {<CRM-NAME3>} {<CRM-NAME4>}	Specifies the critical resource(s) to use with this tunnel • <CRM1-NAME> – Specify the first critical resource name (should be existing). • <CRM-NAME2/3/4> – Optional. Specify the second/third/fourth critical resource names. Maximum of four critical resources can be monitored. **Note:** In case of tunnel initiator, L2TPv3 tunnel is established only if the critical resources identified by the <CRM-NAME1>..... <CRM-NAME4> arguments are available at the time of tunnel establishment. **Note:** In case of L2TPv3 tunnel termination, all incoming tunnel establishment requests are rejected if the critical resources specified by the <CRM-NAME1>..... <CRM-NAME4> arguments are not available.

- `use l2tpv3-policy <L2TPV3-POLICY-NAME>`

use l2tpv3-policy <L2TPV3-POLICY-NAME>	Associates a specified L2TPv3 policy with this tunnel • <L2TPV3-POLICY-NAME> – Specify the policy name (should be existing and configured).

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#use l2tpv3-
policy L2TPV3Policy1

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#show context
 l2tpv3 tunnel Tunnel1
  peer 2 hostname tunnel1peer1 udp port 100
  use l2tpv3-policy L2TPV3Policy1
  session tunnel1peer1session1 pseudowire-id 5000 traffic-source vlan 10-20 native-
vlan 1
  router-id 2000
  establishment-criteria cluster-master
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-tunnel-Tunnel1)#
```

Related Commands

no	Removes the L2TPv3 policy configured with a tunnel and reverts to the default tunnel policy

22.3 l2tpv3-manual-session-commands

L2TPV3-POLICY

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

Use the (profile-context) instance to manually configure a L2TPv3 session. To navigate to the L2TPv3 manual session configuration mode, use the following command in the profile context:

```
<DEVICE>(config-profile-default-rfs7000)#l2tpv3 manual-session <SESSION-NAME>

rfs6000-37FABE(config-profile-default-rfs7000)#l2tpv3 manual-session test
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#?
L2tpv3 Manual Session Mode commands:
  local-cookie        The local cookie for the session
  local-ip-address    Configure the IP address for tunnel. If not specified,
                      tunnel source ip address would be chosen automatically
                      based on the tunnel peer ip address
  local-session-id    Local session id for the session
  mtu                 Configure the mtu size for the tunnel
  no                  Negate a command or set its defaults
  peer                Configure L2TPv3 manual session peer
  remote-cookie       The remote cookie for the session
  remote-session-id   Remote session id for the session
  traffic-source      Traffic that is tunneled

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

The following table summarizes L2TPv3 manual session configuration commands:

Table 22.3 *L2TPV3-Manual-Session-Config Commands*

Command	Description	Reference
local-cookie	Configures the manual session's local cookie field size	*page 22-34*
local-ip-address	Configures the manual session's local source IP address	*page 22-35*
local-session-id	Configures the manual session's local session ID	*page 22-36*
mtu	Configures the MTU size for the manual session tunnel	*page 22-37*
no	Negates or reverts L2TPv3 manual session commands to default	*page 22-23*
peer	Configures the manual session's peers	*page 22-39*
remote-cookie	Configures the remote cookie for the manual session	*page 22-40*

Table 22.3 *L2TPV3-Manual-Session-Config Commands*

Command	Description	Reference
remote-session-id	Configures the manual session's remote session ID	*page 22-41*
traffic-source	Configures the traffic source tunneled by the manual session	*page 22-42*

22.3.1 local-cookie

l2tpv3-manual-session-commands

Configures the local cookie field size for the manual session

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
local-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

Parameters

- `local-cookie size [4|8] <1-4294967295> {<1-4294967295>}`

local-cookie size [4|8]	Configures the local cookie field size for this manual session. The options are: • 4 – 4 byte local cookie field • 8 – 8 byte local cookie field
<1-4294967295>	Configures the local cookie value first word. Applies to both the 4 byte and 8 byte local cookies
<1-4294967295>	Optional – Configures the local cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#local-
cookie size 8 200 300

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Removes the local cookie size configured for a manual session

22.3.2 local-ip-address

l2tpv3-manual-session-commands

Configures the manual session's source IP address. If no IP address is specified, the tunnel's source IP address is automatically configured based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
local-ip-address <IP>
```

Parameters

- `local-ip-address <IP>`

local-ip-address <IP>	Configures the manual session's source IP • <IP> – Specify the IP address in the A.B.C.D format.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test#local-
ip-address 1.2.3.4

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
 local-cookie size 8 200 300
 local-ip-address 1.2.3.4
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Resets the manual session's local source IP address. This re-establishes the session.

22.3.3 local-session-id

l2tpv3-manual-session-commands

Configures the manual session's local session ID

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
local-session-id <1-63>
```

Parameters

- `local-session-id <1-63>`

local-session-id <1-63>	Configures this manual session's local session ID • <1-63> – Specify the ID from 1 - 63. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#local-
session-id 1

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  local-session-id 1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Removes the manual session's local session ID

22.3.4 mtu

l2tpv3-manual-session-commands

Configures the MTU size for the manual session tunnel. The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mtu <128-1460>
```

Parameters

- `mtu <128-1460>`

mtu <128-1460>	Configures the MTU size for this manual session tunnel • <128-1460> – Specify a value from 128 - 1460 bytes (default is 1460 bytes).

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#mtu 200

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  mtu 200
  local-session-id 1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Resets the MTU size for this manual session to default (1460 bytes)

22.3.5 no

l2tpv3-manual-session-commands

Negates or reverts L2TPv3 manual session settings to default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [local-cookie|local-ip-address|local-session-id|mtu|peer|remote-cookie|remote-session-id|traffic-source]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Negates or reverts L2TPv3 manual session settings to default

Example

The following example shows the manual session 'test' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no
local-ip-address
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no
local-session-id
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#no
remote-session-id
```

The following example shows the manual session 'test' settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  remote-cookie size 8 400 700
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

22.3.6 peer

l2tpv3-manual-session-commands

Configures peer(s) allowed to establish the manual session tunnel. The peers are identified by their IP addresses.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
peer ip-address <IP> {udp {port <1-65535>}}
```

Parameters

- `peer ip-address <IP> {udp {port <1-65535>}}`

peer ip-address <IP>	Configures the tunnel's peer IP address in the A.B.C.D format
udp {port <1-65335>}	Optional. Configures the UDP encapsulation mode for this tunnel (default encapsulation is IP) • port <1-65535> – Optional. Configures the peer's UDP port running the L2TPv3 service. • <1-65335> – Specify a value from 1 - 65535.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#peer
ip-address 5.6.7.8 udp port 150

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-cookie size 8 200 300
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  mtu 200
  local-session-id 1
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Removes the manual session's peer

22.3.7 remote-cookie

l2tpv3-manual-session-commands

Configures the manual session's remote cookie field size

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}
```

Parameters

- `remote-cookie size [4|8] <1-4294967295> {<1-4294967295>}`

remote-cookie size [4|8]	Configures the remote cookie field size for this manual session. The options are: • 4 – 4 byte remote cookie field • 8 – 8 byte remote cookie field
<1-4294967295>	Configures the remote cookie value first word. Applies to both the 4 byte and 8 byte local cookies
<1-4294967295>	Optional – Configures the remote cookie value second word. Applicable to only 8 byte cookies. This parameter is ignored for 4 byte cookies.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#remote-
cookie size 8 400 700

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  mtu 200
  local-session-id 1
  remote-cookie size 8 400 700
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Removes the manual session's remote cookie field size

22.3.8 remote-session-id

l2tpv3-manual-session-commands

Configures the manual session's remote ID. This ID is passed in the establishment of the tunnel session.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
remote-session-id <1-4294967295>
```

Parameters

- `remote-session-id <1-4294967295>`

remote-session-id <1-4294967295>	Configures this manual session's remote ID • <1-4294967295> – Specify a value from 1 - 4294967295.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#remote-
session-id 200

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Removes the manual session's remote ID

22.3.9 traffic-source

l2tpv3-manual-session-commands

Configures the traffic source tunneled by this session

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}
```

Parameters

- `traffic-source vlan <VLAN-ID-RANGE> {native-vlan <1-4094>}`

traffic-source vlan <VLAN-ID-RANGE>	Configures VLAN as the traffic source for this tunnel • <VLAN-ID-RANGE> – Configures VLAN range list of traffic source. Specify the VLAN IDs as a range (for example, 10-20, 25, 30-35)
native-vlan <1-4094>	Optional – Configures the native VLAN ID for this session, which is not tagged • <1-4094> – Specify the native VLAN ID from 1- 4094.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-
test)#traffic-source vlan 50-60 native-vlan 2

rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#show
context
 l2tpv3 manual-session test
  local-ip-address 1.2.3.4
  peer ip-address 5.6.7.8 udp port 150
  traffic-source vlan 50-60 native-vlan 2
  local-session-id 1
  remote-session-id 200
  remote-cookie size 8 400 700
rfs6000-37FABE(config-profile default-rfs7000-l2tpv3-manual-session-test)#
```

Related Commands

no	Removes the traffic source configured for a tunnel

23 ROUTER-MODE COMMANDS

This chapter summarizes *Open Shortest Path First* (OSPF) router mode commands in the CLI command structure. All router-mode commands are available on both device and profile modes.

OSPF is an *interior gateway protocol* (IGP) used within large autonomous systems to distribute routing information. OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer, which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers. This enables routers to synchronize routing tables.

OSPF uses a route table managed by the link cost (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability.

Use the (config) instance to configure router commands. To navigate to the (config-router-mode) instance, use the following command:

```
<DEVICE>(config-profile-<PROFILE-NAME>)#router ospf
<DEVICE>(config-profile <PROFILE-NAME>-router-ospf)#

rfs6000-37FABE(config-profile-default-rfs7000)#router ospf
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#?
Router OSPF Mode commands:
  area                  OSPF area
  auto-cost             OSPF auto-cost
  default-information   Distribution of default information
  ip                    Internet Protocol (IP)
  network               OSPF network
  no                    Negate a command or set its defaults
  ospf                  OSPF
  passive               Make OSPF Interface as passive
  redistribute          Route types redistributed by OSPF
  route-limit           Limit for number of routes handled OSPF process
  router-id             Router ID

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  do                    Run commands from Exec mode
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

23.1 router-mode

- *ROUTER-MODE COMMANDS*

The following table summarizes router configuration commands:

Table 23.1 *OSPF-Router Config Commands*

Command	Description	Reference
area	Specifies OSPF enabled interfaces	*page 23-3*
auto-cost	Specifies the reference bandwidth in terms of Mbits per second	*page 23-12*
default-information	Controls the distribution of default information	*page 23-13*
ip	Configures *Internet Protocol* (IP) default gateway priority	*page 23-14*
network	Defines OSPF network settings	*page 23-15*
ospf	Enables OSPF	*page 23-16*
passive	Specifies the configured OSPF interface as passive interface	*page 23-17*
redistribute	Specifies the route types redistributed by OSPF	*page 23-18*
route-limit	Specifies the limit for the number of routes managed by OSPF	*page 23-19*
router-id	Specifies the router ID for OSPF	*page 23-21*
no	Negates a command or sets its defaults	*page 23-22*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

23.1.1 area

router-mode

Configures OSPF network area (OSPF enabled interfaces) settings

The following table lists the OSPF Area configuration mode commands:

Table 23.2 *OSPF Area Config Commands*

Command	Description	Reference
area	Creates a new OSPF area and enters its configuration mode	*page 23-4*
OSPF-area-mode	Summarizes OSPF area configuration commands	*page 23-6*

23.1.1.1 area

area

Configures OSPF network areas (OSPF enables interfaces)

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can defined as: *stub area*, *totally-stub*, *non-stub*, *nssa*, *totally nssa*. Each of these area types have been discussed further in the *area-type* section of this chapter.

At least one default area, bearing number '0', should be configured for every OSPF network. In case of multiple areas, the default area 0 forms the backbone of the network. The default area 0 is used as a link to the other areas. Each area has its own link-state database.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
area [<0-4294967295>|<IP>]
```

Parameters

- `area [<0-4294967295>|<IP>]`

area	Defines an OSPF area
<0-4294967295>	Defines an OSPF area in the form of a 32 bit integer • <0-4294967295> – Specify the value from 0 - 4294967295.
<IP>	Defines an OSPF area in the form of an IP address • <IP> – Specify the IP address.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#area 4 ?
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#?
Router OSPF Area Mode commands:
  area-type       OSPF area type
  authentication  Authentication scheme for OSPF area
  no              Negate a command or set its defaults
  range           Routes matching this range are considered for summarization
                  (ABR only)

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
```

```
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#

rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#show
context
  area 0.0.0.4
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.4)#
```

Related Commands

no	Removes area configuration settings

23.1.1.2 OSPF-area-mode

- *area*

The following table summarizes OSPF area mode configuration commands:

Table 23.3 *OSPF-Area-Mode Commands*

Command	Description	Reference
area-type	Configures a particular OSPF area as STUB or NSSA	*page 23-7*
authentication	Specifies the authentication scheme used for the OSPF area	*page 23-9*
range	Specifies the routes matching address/mask for summarization	*page 23-10*
no	Negates a command or sets its defaults	*page 23-11*

23.1.1.2.1 area-type

OSPF-area-mode

Configures a particular OSPF area type as STUB, Totally STUB, NSSA or Totally NSSA

Areas can be defined as:

- stub area - Is an area that does not receive route advertisements external to the *autonomous system* (AS), and routing from within the area is based entirely on a default route.
- totally-stub - Is an area that does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there is only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- non-stub - Is an area that imports autonomous system external routes and forwards to other areas. However. it still cannot receive external routes from other areas.
- nssa - A *Not-So-Stubby Area* (NSSA) is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.
- totally-nssa - Is a NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an *Autonomous System Boundary Router* (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
area-type [nssa|stub]

area-type nssa {default-cost|no-summary|translate-always|translate-candidate|
translate-never}

area-type nssa {default-cost <0-16777215> {no-summary}|no-summary {default-cost
<0-16777215>}}

area-type nssa {translate-always|translate-candidate|translate-never} {(default-
cost <0-16777215>|no-summary)}

area-type stub {default-cost <0-16777215> {no-summary}|no-summary {default-cost
<0-16777215>}}
```

Parameters

```
• area-type [nssa|stub]{default-cost|no-summary|translate-always|translate-
candidate|translate-never}
```

area-type	Configures a particular OSPF area type as STUB, Totally STUB, NSSA or Totally NSSA
nssa	Configures the OSPF area as NSSA
stub	Configures the OSPF area as *Stubby Area* (STUB)
default-cost <0-16777215>	Specifies the default summary cost that will be advertised, if the OSPF area is a STUB or NSSA • <0-16777215> – Specify the default summary cost value from 0 - 16777215.

no-summary	Configures the OSPF area as totally STUB if the area-type is STUB or totally NSSA if the area-type is NSSA
translate-always	Always translates type-7 *Link State Advertisements* (LSAs) into type-5 LSAs
translate-candidate	Defines it as default behavior
translate-never	Never translates type-7 LSAs into type-5 LSAs

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#area-type
stub default-cost 1

rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   area-type stub default-cost 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands

no	Removes configured area-type settings

23.1.1.2.2 authentication

OSPF-area-mode

Specifies an authentication scheme used for an OSPF area used with the OSPF dynamic route

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
authentication [message-digest|simple-password]
```

Parameters

- `authentication [message-digest|simple-password]`

message-digest	Configures the message-digest (MD-5) authentication scheme
simple-password	Configures the simple password authentication scheme

Usage Guidelines

OSPF packet authentication enables routers to use predefined passwords and participate within a routing domain. The two authentication modes are:

- MD-5 – MD-5 authentication is a cryptographic authentication mode, where every router has a key (password) and key-id configured on it. This key and key-id together form the message digest that is appended to the OSPF packet.
- Simple Password – Simple password authentication allows a password (key) to be configured per area. Routers in the same area and participating in the routing domain have to be configured with the same key.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-
0.0.0.1)#authentication simple-password

rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   authentication simple-password
   area-type stub default-cost 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands

no	Removes the authentication scheme

23.1.1.2.3 range

OSPF-area-mode

Specifies a range of addresses for routes matching address/mask for OSPF summarization

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
range <IP/M>
```

Parameters

- `range <IP/M>`

<IP/M>	Specifies the routes matching address/mask for summarization. **Note:** This command is applicable for a *Area Border Router* (ABR) only.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#range
172.16.10.0/24

rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   authentication simple-password
   range 172.16.10.0/24
   area-type stub default-cost 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

Related Commands

no	Removes the configured network IP range

23.1.1.2.4 no

OSPF-area-mode

Negates a command or set its defaults

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
no [area-type|authentication|range]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or set its defaults

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example shows the OSPF router settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   authentication simple-password
   range 172.16.10.0/24
   area-type stub default-cost 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#

rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#no
authentication
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#no range
 172.16.10.0/24
```

The following example shows the OSPF router settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#show
context
  area 0.0.0.1
   area-type stub default-cost 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf-area-0.0.0.1)#
```

23.1.2 auto-cost

router-mode

Configures the reference bandwidth in terms of megabits per second. Specifying the reference bandwidth allows you to control the default metrics for an interface, which is calculated by OSPF.

The formula used to calculate default metrics is: *ref-bw* divided by the *bandwidth*.

Use the '*no > auto-cost > reference-bandwidth*' command to configure default metrics calculation based on interface type.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602. AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
auto-cost reference-bandwidth <1-4294967>
```

Parameters

- `auto-cost reference-bandwidth <1-4294967>`

reference-bandwidth <1-4294967>	Defines the reference bandwidth in Mbps • <1-4294967> – Specify the reference bandwidth value from1 - 4294967.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#auto-cost reference-
bandwidth 1
```

Ensure that the auto-cost reference-bandwidth is configured uniformly on all routers.

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  area 0.0.0.4
  auto-cost reference-bandwidth 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Removes auto-cost reference bandwidth settings

23.1.3 default-information

router-mode

Controls the distribution of default route information. Use the *default-information > originate* command to advertise a default route in the routing table.

This option is disabled by default. When enabled, the default route becomes a distributed route.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
default-information originate {always|metric|metric-type}
default-information originate {always|metric <0-16777214>|metric-type [1|2]}
{(metric <0-16777214>|metric-type [1|2])}
```

Parameters

- `default-information originate {always|metric <0-16777214>|metric-type [1|2]} {(metric <0-16777214>|metric-type [1|2])}`

originate	Originates default route information. Enabling this feature makes the default route a distributed route. This option is disabled by default.
always	Optional. Always distributes default route information (will continue to advertise default route information even if that information has been removed from the routing table for some reason). This option is disabled by default.
metric <0-16777214>	This is a recursive parameter and can be optionally configured along with the metric-type option. • metric <0-16777214> – Optional. Specifies OSPF metric value for redistributed routes (this value is used to generate the default route) • <0-16777214> – Specify a value from 0 - 16777214.

metric-type [1|2]	This is a recursive parameter and can be optionally configured along with the metric option.
	• metric-type [1|2] – Optional. Sets OSPF exterior metric type for redistributed routes (this information is advertised with the OSPF routing domain)
	  • 1 – Sets OSPF external type 1 metrics
	  • 2 – Sets OSPF external type 2 metrics

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#default-information
originate metric-type 2 metric 1

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Disables advertising of default route information available in the routing table

23.1.4 ip

router-mode

Configures IP default gateway priority

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
ip default-gateway priority <1-8000>
```

Parameters

- `ip default-gateway priority <1-8000>`

default-gateway	Configures the default gateway
priority <1-8000>	Sets the priority for the default gateway acquired via OSPF • <1-8000> – Specify an integer from 1 - 8000. The default is 7000. **Note:** Lower the value, higher is the priority.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#ip default-gateway
priority 1

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Removes default gateway priority settings

23.1.5 network

router-mode

Assigns networks to specified areas (defines the OSPF interfaces and their associated area IDs)

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
network <IP/M> area [<0-4294967295>|<IP>]
```

Parameters

- `network <IP/M> area [<0-4294967295>|<IP>]`

<IP/M>	Specifies an OSPF network address/mask value. Defines networks (IP addresses and mask) participating in OSPF.
area [<0-4294967295>|<IP>]	Specifies an OSPF area, associated with the OSPF address range, in one of the following formats: • <0-4294967295> – Specifies a 32 bit OSPF area ID from 0 - 4294967295 • <IP> – Defines an OSPF area ID in the form of an IPv4 address

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#network 1.2.3.0/24
area 4.5.6.7

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Removes the OSPF network to area ID association

23.1.6 ospf

router-mode

Enables OSPF routing on a profile or device

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
ospf enable
```

Parameters

- `ospf enable`

ospf enable	Enables OSPF routing on devices using this profile. This option is disabled by default.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#ospf enable

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Disables OSPF routing on a profile or device

23.1.7 passive

router-mode

Configures specified OSPF interface as passive. This option is disabled by default.

A passive interface receives routing updates, but does not transmit them.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
passive [<WORD>|all|vlan <1-4094>]
```

Parameters

- `passive [<WORD>|all|vlan <1-4094>]`

<WORD>	Enables the OSPF passive mode on the interface specified by the <WORD> parameter
all	Enables the OSPF passive mode on all the L3 interfaces
vlan <1-4094>	Enables the OSPF passive mode on the specified VLAN interface • <1-4094> – Specify the VLAN interface ID from 1 - 4094.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#passive vlan 1

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  passive vlan1
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Disables the OSPF passive mode on a specified interface

23.1.8 redistribute

router-mode

Specifies the route types redistributed by OSPF

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
redistribute [bgp|connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}
```

Parameters

- `redistribute [connected|kernel|static] {metric <0-16777214>|metric-type [1|2]}`

bgp	Redistributes all BGP routes by OSPF
connected	Redistributes all connected interface routes by OSPF
kernel	Redistributes all routes that are neither connected, static, dynamic, nor bgp
static	Redistributes static routes by OSPF
metric <0-16777214>	The following keywords are common to the 'bgp', 'connected', 'kernel', and 'static' parameters: • metric <0-16777214> – Optional. Specifies the OSPF metric value for redistributed routes. • <0-16777214> – Specify a value from 0 - 16777214.

metric-type [1|2]	The following keywords are common to the 'connected', 'kernel', and 'static' parameters:
	• metric-type [1|2] – Optional. Sets the OSPF exterior metric type for redistributed routes
	  • 1 – Sets the OSPF external type 1 metrics
	  • 2 – Sets the OSPF external type 2 metrics

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#redistribute static
metric-type 1

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Removes the OSPF redistribution of various route types

23.1.9 route-limit

router-mode

Limits the number of routes managed by OSPF. The maximum limit supported by the platform is the default configuration defined under the router-ospf context.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
route-limit [num-routes|reset-time|retry-count|retry-timeout]

route-limit [num-routes <DYNAMIC-ROUTE-LIMIT>|reset-time <1-86400>|retry-count
<1-32>|retry-timeout <1-3600>] {(num-routes|reset-time|retry-count|retry-
timeout)}
```

Parameters

```
• route-limit [num-routes <DYNAMIC-ROUTE-LIMIT>|reset-time <1-86400>|retry-count
<1-32>|retry-timeout <1-3600>] {(num-routes|reset-time|retry-count|retry-
timeout)}
```

num-routes <DYNAMIC-ROUTE-LIMIT>	Specifies the maximum number of non self-generated LSAs this process can receive • <DYNAMIC-ROUTE-LIMIT> – Specify the dynamic route limit.
reset-time <1-86400>	Specifies the time, in seconds, after which the retry-count is reset to zero <1-86400> – Specify a value from 1 - 86400 seconds. The default is 360 seconds.
retry-count <1-32>	Specifies the maximum number of times adjacencies can be suppressed. Each time OSPF gets into an ignore state, a counter increments. If the counter exceeds the timeout configured by the retry-count parameter, OSPF stays in the same ignore state. Manual intervention is required to get OSPF out of the ignore state. • <1-32> – Specify a value from 1 - 32. The default is 5.
retry-timeout <1-3600>	Specifies the retry time in seconds. During this time, OSPF remains in ignore state and all adjacencies are suppressed. • <1-3600> – Specify a value from 1 - 3600 seconds. The default is 60 seconds.

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#route-limit num-routes
10 retry-count 5 retry-timeout 60 reset-time 10

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  ospf enable
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 retry-count 5 retry-timeout 60 reset-time 10
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Removes the limit on the number of routes managed by OSPF

23.1.10 router-id

router-mode

Specifies the OSPF router ID

This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
router-id <IP>
```

Parameters

- `router-id <IP>`

<IP>	Identifies the OSPF router by its IP address • <IP> – Specify the router ID in the IP <A.B.C.D> format

Example

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#router-id 172.16.10.8
Reload, or execute "clear ip ospf process" command, for this to take effect
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

Related Commands

no	Removes the configured OSPF router ID

23.1.11 no

router-mode

Negates a command or reverts settings to their default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7622, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000

Syntax

```
no [area|auto-cost|default-information|ip|network|ospf|passive|redistribute|
route-limit|router-id]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or set its defaults

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example shows the OSPF router interface settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  network 1.2.3.0/24 area 4.5.6.7
  area 0.0.0.4
  auto-cost reference-bandwidth 1
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 reset-time 10
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#

rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#no area 4
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#no auto-cost
reference-bandwidth
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#no network 1.2.3.0/24
area 4.5.6.7
```

The following example shows the OSPF router interface settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#show context
 router ospf
  default-information originate metric 1 metric-type 2
  redistribute static metric-type 1
  passive vlan1
  route-limit num-routes 10 reset-time 10
  ip default-gateway priority 1
rfs6000-37FABE(config-profile default-rfs7000-router-ospf)#
```

24 ROUTING-POLICY

This chapter summarizes routing-policy commands in the CLI command structure.

Routing policies enable network administrators to control data packet routing and forwarding. *Policy-based routing* (PBR) always overrides protocol-based routing. Network administrators can define routing policies based on parameters, such as access lists, packet size, etc. For example, a routing policy can be configured to route packets along user-defined routes.

In addition to the above, PBR facilitates the provisioning of preferential service to specific traffic. PBR minimally provides the following:

- A means to use source address, protocol, application, and traffic class as traffic routing criteria
- A means to load balance multiple WAN uplinks
- A means to selectively mark traffic for *Quality of Service* (QoS) optimization

Use the (config) instance to configure router-policy commands. To navigate to the (config-routing-policy mode) instance, use the following commands:

```
<DEVICE>(config)#routing-policy <ROUTING-POLICY-NAME>
```

```
rfs6000-37FABE(config)#routing-policy testpolicy
rfs6000-37FABE(config-routing-policy-testpolicy)#?
Routing Policy Mode commands:
  apply-to-local-packets  Use Policy Based Routing for packets generated by
                          the device
  logging                 Enable logging for this Route Map
  no                      Negate a command or set its defaults
  route-map               Create a Route Map
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs6000-37FABE(config-routing-policy-testpolicy)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

24.1 routing-policy-commands

ROUTING-POLICY

The following table summarizes routing policy configuration commands:

Table 24.1 *Routing-Policy-Config Commands*

Command	Description	Reference
apply-to-local-packets	Enables PBR for locally generated packets	*page 24-3*
logging	Enables logging for a specified route map	*page 24-4*
route-map	Creates a route map entry	*page 24-5*
use	Defines default settings to use	*page 24-18*
no	Negates a command or sets its defaults	*page 24-19*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

24.1.1 apply-to-local-packets

routing-policy-commands

Enables PBR for locally generated packets (packets generated by the device). When enabled, this option implements the match and action clauses defined within route maps. This option is enabled by default.

To disable PBR, use the *no > apply-to-local-packets* command.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
apply-to-local-packets
```

Parameters

None

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy)#apply-to-local-packets
rfs6000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands

no	Disables PBR for locally generated packets

24.1.2 logging

routing-policy-commands

Enables logging for a specified route map. When enabled, this option logs events generated by the enforcement of route-maps. This option is disabled by default.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
logging
```

Parameters

None

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy)#logging

rfs6000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
rfs6000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands

no	Disables route map logging

24.1.3 route-map

routing-policy-commands

Creates a route map entry and enters the route map configuration mode

In *policy-based routing* (PBR), route maps control the flow of traffic within the network. They override route tables and direct traffic along a specific path.

Route-maps contain a set of filters that select traffic (*match* clauses) and associated actions (*mark* clauses) for routing. Every route-map entry has a precedence value. Lower the precedence, higher is the route-map's priority. All incoming packets are matched against these route-maps entries. The route-map entry with highest precedence (lowest numerical value) is applied first. In case of a match, action is taken based on the mark clause specified in the route-map. In case of no match, the route-map entry with the next highest precedence is applied. If the incoming packet does not match any of the route-map entries, it is subjected to typical destination-based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- *IP Access List* - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

  - *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP *Differentiated Services Code Point* (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.
  - *Incoming WLAN* - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:

- Device *with* an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
- Device *without* an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.
  - *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
  - *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

Mark (or action) clauses determine the routing function when a packet satisfies match criteria. If no mark clauses are defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped. The mark clause defines one of following actions:

- *Next hop* - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used. But if all next hops are unreachable, typical destination-based route lookup is performed.

- *Default next hop* - If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This can be either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the *next hop* and the *default next-hop* is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reversed. In both cases:

a If a defined next hop is reachable, it is used. If fallback is configured refer to (b).

b Perform normal destination-based route lookup. If a next hop is found, it is used, if not refer to (c).

c If default next hop is configured and reachable, it is used, if not, packet is dropped.

- *Fallback* - Enables fallback to destination-based routing if none of the configured next hops are reachable (or not configured). This is enabled by default.
- *Mark IP DSCP* - Configures IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
route-map <1-100>
```

Parameters

- `route-map <1-100>`

route-map <1-100>	Creates a route map entry, sets a precedence value for the route map, and enters the route map configuration mode • <1-100> – Specify a precedence value from 1 - 100. **Note:** Lower the sequence number, higher is the precedence.

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy)#route-map 1

rfs6000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
 route-map 1
rfs6000-37FABE(config-routing-policy-testpolicy)#

rfs6000-37FABE(config-routing-policy-testpolicy)#route-map 1
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#?
Route Map Mode commands:
  default-next-hop  Default next-hop configuration (aka
                    gateway-of-last-resort)
  fallback          Fallback to destination based routing if no next-hop is
                    configured or all are unreachable
  mark              Mark action for route map
  match             Match clause configuration for Route Map
  next-hop          Next-hop configuration
  no                Negate a command or set its defaults

  clrscr            Clears the display screen
  commit            Commit all changes made in this session
  do                Run commands from Exec mode
  end               End current mode and change to EXEC mode
  exit              End current mode and down to previous mode
  help              Description of the interactive help system
```

```
  revert            Revert changes
  service           Service Commands
  show              Show running system information
  write             Write running configuration to memory or terminal

rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

no	Removes a route map

24.1.4 route-map-mode

route-map

The following table summarizes route-map configuration commands:

Table 24.2 *Route-Map-Config Commands*

Command	Description	Reference
default-next-hop	Sets the default next hop for packets satisfying match criteria	*page 24-9*
fallback	Configures a fallback to the next destination	*page 24-10*
mark	Marks action clause for packets satisfying match criteria	*page 24-11*
match	Sets match clauses for the route map	*page 24-12*
next-hop	Sets the next hop for packets satisfying match criteria	*page 24-15*
no	Negates a command or sets its default	*page 24-17*

24.1.4.1 default-next-hop

route-map-mode

Sets the default next hop for packets satisfying match criteria

If a packet, subjected to PBR, does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is: in case of the former, PBR occurs first, then destination-based routing. In case of the latter, the order is reverse. Use this command to set either the default next hop IP address or define either a WWAN1, PPPoE1, or VLAN interface.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7562, AP7602, AP7612, AP7622, AP7632, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
default-next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]
```

Parameters

```
• default-next-hop [<IP>|<ROUTER-IF-NAME>|serial <SLOT-ID> <PORT-ID> <CHANNEL-
GROUP-ID>|pppoe1|vlan <1-4094>|wwan1]
```

default-next-hop	Sets the next hop router to which packets are sent in case the next hop is not the adjacent router
<IP>	Specifies next hop router's IP address
<ROUTER-IF-NAME>	Specifies the outgoing interface name (router interface name)
pppoe1	Specifies the PPPoE interface
serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>	Specifies the serial interface's slot, port, and channel group IDs
vlan <1-4094>	Specifies a VLAN interface ID • <1-4094> – Specify a value from 1 - 4094.
wwan1	Specifies the WAN interface

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#default-next-hop
wwan1

rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  default-next-hop wwan1
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

no	Removes default next hop router settings

24.1.4.2 fallback

route-map-mode

Enables fallback to destination-based routing. This option is enabled by default. To disable fallback, use the *no > fallback* command.

The action taken for packets satisfying the match criteria is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing.

NOTE: If no mark clause is configured and fallback to destination-based routing is disabled, then the packet is dropped.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
fallback
```

Parameters

None

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#fallback
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

no	Disables fallback to destination-based routing, if no next hop is configured or are unreachable

24.1.4.3 mark

route-map-mode

Enables the marking of the DSCP field in the IP header

Use this command to set the IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

The DSCP field in an IP header enables packet classification. Packet filtering can be done based on traffic class, determined from the IP DSCP field. One DSCP value can be configured per route map entry.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
mark ip dscp <0-63>
```

Parameters

- `mark ip dscp <0-63>`

ip dscp <0-63>	Marks the DSCP field in the IP header • <0-63> – Specify a DSCP value from 0 - 63.

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#mark ip dscp 7

rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  default-next-hop wwan1
  mark ip dscp 7
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

no	Disables marking of IP packets

24.1.4.4 match

route-map-mode

Sets the match clauses

Each route map entry has a set of *match* clauses used to segregate and filter packets. Packets can be segregated using any one of the following criteria:

- *IP Access List* - A typical IP ACL can be used for routing traffic. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP *Differentiated Services Code Point* (DSCP) field. One DSCP value can be configured per route map entry. If IP ACLs on a WLAN, ports or SVI mark packets, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered on the basis of the incoming WLAN. Depending on whether the receiving device has an onboard radio or not, the following two scenarios are possible:

- Device *with* an onboard radio: If a device having an onboard radio and capable of PBR receives a packet on a local WLAN, this WLAN is used for selection.
- Device *without* an onboard radio: If a device, without an onboard radio, capable of PBR receives a packet from an extended VLAN, it passes the WLAN information in the MiNT packet to the PBR router. The PBR router uses this information as match criteria.
  - *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
  - *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the source host (where the packet originates) is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing PBR, and not to the source device.

The action taken for filtered packets is determined by the mark (action) clauses. If no action is defined, the default is to fallback to destination-based routing for packets satisfying the match criteria. For more information on configuring mark clauses, see *mark*. And for more information on fallback action, see *fallback*.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
match [incoming-interface|ip|ip-access-list|wireless-client-role|wlan]

match incoming-interface [<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID>
<CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]

match ip dscp <0-63>
```

```
match ip-access-list <IP-ACCESS-LIST-NAME>

match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>

match wlan <WLAN-NAME>
```

Parameters

- `match incoming-interface [<ROUTER-IF-NAME>|pppoe1|serial<SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwan1]`

incoming-interface	Sets the incoming SVI match clause. Specify an interface name.
<ROUTER-IF-NAME>	Specifies the layer 3 interface name (route interface)
pppoe1	Specifies the PPP over Ethernet interface
serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>	Specifies the serial interface's slot, port, and channel group IDs.
vlan <1-4094>	Specifies the VLAN interface ID • <1-4094> – Specify a VLAN ID from 1 - 4094.
wwan1	Specifies the WAN interface name

- `match ip dscp <0-63>`

ip dscp <0-63>	Sets the DSCP match clause • <0-63> – Specify a value from 0 - 63. The defined DSCP value is used as a matching clause for this route map.

- `match ip-access-list <IP-ACCESS-LIST-NAME>`

ip-access-list <IP-ACCESS-LIST-NAME>	Sets the match clause using a pre-configured IP access list • <IP-ACCESS-LIST-NAME> – Specify a pre-configured IP access list name.

- `match wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>`

wireless-client-role <ROLE-POLICY-NAME> <ROLE-NAME>	Sets the wireless client role match clause • <ROLE-POLICY-NAME> – Specify a pre-configured role policy. • <ROLE-NAME> – Specify a pre-configured role within it.

- `match wlan <WLAN-NAME>`

wlan <WLAN-NAME>	Sets the incoming WLAN match clause • <WLAN-NAME> – Specify a WLAN name.

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#match incoming-
interface pppoe1

rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  default-next-hop wwan1
  mark ip dscp 7
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

no	Disables match clause settings for this route map

24.1.4.5 next-hop

route-map-mode

Sets the next hop for packets satisfying match criteria

This command allows you to configure the primary and secondary hop priority requests.

Define the primary and secondary hop settings. When defined, the primary hop resource is used with no additional considerations when ever it is available.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwlan1] {<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwlan1}
```

Parameters

```
• next-hop [<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwlan1] {<IP>|<ROUTER-IF-NAME>|pppoe1|serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>|vlan <1-4094>|wwlan1}
```

next-hop	Sets the next hop (primary and secondary) for packets satisfying match criteria It is not mandatory to define the secondary hop interface. The secondary hop is used in case the primary hop is unavailable.
<IP>	Specifies the primary and secondary next hop router's IP address
<WORD>	Specifies the layer 3 Interface name (router interface)
pppoe1	Specifies the PPP over Ethernet interface
serial <SLOT-ID> <PORT-ID> <CHANNEL-GROUP-ID>	Specifies the serial interface's slot, port, and channel group IDs.
vlan <1-4094>	Specifies the VLAN interface ID • <1-4094> – Specify a VLAN ID from 1 - 4094. The VLAN interface should be a DHCP client.
wwan1	Specifies the WAN interface

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#next-hop vlan 1

rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  next-hop vlan1
  default-next-hop wwan1
  mark ip dscp 7
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

Related Commands

no	Disables the next hop router settings

24.1.4.6 no

route-map-mode

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [default-next-hop|fallback|mark|match|next-hop]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or set its defaults

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example shows the route-map '1' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  next-hop vlan1
  default-next-hop wwan1
  mark ip dscp 7
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#

rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#no default-next-hop
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#no next-hop
```

The following example shows the route-map '1' settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#show context
 route-map 1
  match incoming-interface pppoe1
  mark ip dscp 7
rfs6000-37FABE(config-routing-policy-testpolicy-route-map-1)#
```

24.1.5 use

routing-policy-commands

Uses *Critical Resource Management* (CRM) to monitor link status

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use critical-resource-monitoring
```

Parameters

- `use critical-resource-monitoring`

use critical-resource-monitoring	Uses CRM to monitor the status of a link. Selecting this option determines the disposition of the route-map next hop via monitored critical resources. Link monitoring is the function used to determine a potential fail over to the secondary next hop. This option is enabled by default.

Example

```
rfs6000-37FABE(config-routing-policy-testpolicy)#use critical-resource-monitoring
rfs6000-37FABE(config-routing-policy-testpolicy)#
```

Related Commands

no	Disables CRM link status monitoring

24.1.6 no

routing-policy-commands

Negates a command or sets its defaults

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [apply-to-local-packets|logging|route-map|use]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Negates a command or set its defaults

Usage Guidelines

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

The following example shows the routing policy 'testpolicy' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 logging
 route-map 1
  match incoming-interface pppoe1
  default-next-hop wwan1  mark ip dscp 7
rfs6000-37FABE(config-routing-policy-testpolicy)#

rfs6000-37FABE(config-routing-policy-testpolicy)#no logging
rfs6000-37FABE(config-routing-policy-testpolicy)#no route-map 1
rfs6000-37FABE(config-routing-policy-testpolicy)#no apply-to-local-packets
```

The following example shows the routing policy 'testpolicy' settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-routing-policy-testpolicy)#show context
routing-policy testpolicy
 no apply-to-local-packets
rfs6000-37FABE(config-routing-policy-testpolicy)#
```

25 AAA-TACACS-POLICY

This chapter summarizes the *accounting, authentication, and authorization* (AAA) *Terminal Access Control Access-Control System* (TACACS) policy commands in the CLI command structure.

TACACS is a network security application that provides additional network security by providing a centralized authentication, authorization, and accounting platform. TACACS implementation requires configuration of the TACACS authentication server and database.

Use the (config) instance to configure AAA-TACACS policy commands. To navigate to the config-aaa-tacacs-policy instance, use the following commands:

```
<DEVICE>(config)#aaa-tacacs-policy <POLICY-NAME>

rfs6000-37FABE(config)#aaa-tacacs-policy test
rfs6000-37FABE(config-aaa-tacacs-policy-test)#?
AAA TACACS Policy Mode commands:
  accounting      Configure accounting parameters
  authentication  Configure authentication parameters
  authorization   Configure authorization parameters
  no              Negate a command or set its defaults

  clrscr          Clears the display screen
  commit          Commit all changes made in this session
  do              Run commands from Exec mode
  end             End current mode and change to EXEC mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  write           Write running configuration to memory or terminal

rfs6000-37FABE(config-aaa-tacacs-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

25.1 aaa-tacacs-policy

- *AAA-TACACS-POLICY*

The following table summarizes AAA-TACACS policy configuration commands:

Table 25.1 *AAA-TACACS-Policy-Config Commands*

Command	Description	Reference
accounting	Configures TACACS accounting parameters	*page 25-3*
authentication	Configures TACACS authentication parameters	*page 25-6*
authorization	Configures TACACS authorization parameters	*page 25-9*
no	Negates a command or sets its default	*page 25-12*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

25.1.1 accounting

aaa-tacacs-policy

Configures the server type and interval at which interim accounting updates are sent to the server. Up to 2 accounting servers can be configured.

This feature tracks user activities on the network, and provides information such as, resources used and usage time. This information can be used for audit and billing purposes.

TACACS accounting tracks user activity and is useful for security audit purposes.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
accounting [access-method|auth-fail|commands|server|session]

accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}

accounting [auth-fail|commands|session]

accounting server [<1-2>|preference]

accounting server preference [authenticated-server-host|authenticated-server-
number|authorized-server-host|authorized-server-number|none]

accounting server <1-2> [host|retry-timeout-factor <50-200>|timeout]

accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}

accounting server <1-2> timeout <3-5> {attempts <1-3>}
```

Parameters

- `accounting access-method [all|console|ssh|telnet] {(console|ssh|telnet)}`

access-method	Configures TACACS accounting access mode. The options are: console, SSH, Telnet, and all.
all	Configures TACACS accounting for all access modes
console	Configures TACACS accounting for console access only
ssh	Configures TACACS accounting for SSH access only
telnet	Configures TACACS accounting for Telnet access only

- `accounting [auth-fail|commands|session]`

auth-fail	Enables accounting for authentication fail details. This option is disabled by default.
commands	Enables accounting of commands executed. This option is disabled by default.
session	Enables accounting for session start and stop details. This option is disabled by default.

- `accounting server preference [authenticated-server-host|authenticated-server-number|authorized-server-host|authorized-server-number|none]`

server	Configures a TACACS accounting server
preference	Configures the accounting server preference (specifies the method of selecting a server, from the pool, to send the request)
authenticated-server-host	Sets the authentication server as the accounting server. This is the default setting. This parameter indicates the same server is used for authentication and accounting. The server is referred to by its hostname.
authenticated-server-number	Sets the authentication server as the accounting server This parameter indicates the same server is used for authentication and accounting. The server is referred to by its index or number.
authorized-server-host	Sets the authorization server as the accounting server This parameter indicates the same server is used for authorization and accounting. The server is referred to by its hostname.
authorized-server-number	Sets the authorized server as the accounting server This parameter indicates the same server is used for authorization and accounting. The server is referred to by its index number.
none	Indicates the accounting server is independent of the authentication and authorization servers

- `accounting server <1-2> retry-timeout-factor <50-200>`

server <1-2>	Configures an accounting server. Up to 2 accounting servers can be configured
retry-timeout-factor <50-200>	Sets the scaling factor for retry timeouts • <50-200> – Specify a value from 50 - 200. The default is 100. A value of 100 indicates the time gap between two consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the time gap between two consecutive retries reduces with each successive retry. A value greater than 100 indicates the time gap between two consecutive retries increases with each successive retry.

- `accounting server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}`

server <1-2>	Configures an accounting server. Up to 2 accounting servers can be configured
host <IP/HOSTNAME>	Configures the accounting server's IP address or hostname
secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Optional. Configures a common secret key used to authenticate with the accounting server • 0 <SECRET> – Configures a clear text secret key • 2 <SECRET> – Configures an encrypted secret key • <SECRET> – Specify the secret key. This shared secret should not exceed 127 characters.
port <1-65535>	Optional. Configures the accounting server port (the port used to connect to the accounting server) • <1-65535> – Specify the TCP accounting port number from 1 - 65535. The default port is 49.

- `accounting server <1-2> timeout <3-5> {attempts <1-3>}`

server <1-2>	Configures an accounting server. Up to 2 accounting servers can be configured
timeout <3-5>	Configures the timeout for each request sent to the TACACS accounting server. This is the time allowed to elapse before another request is sent to the TACACS accounting server. If a response is received from the server within this time, no retry is attempted. • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.
attempts <1-3>	Optional. Specifies the number of times a transmission request is attempted. This is the maximum number of times a request is sent to the TACACS accounting server before getting discarded. • <1-3> – Specify a value from 1 - 3. The default is 3.

Example

```
rfs6000-37FABE(config-aaa-tacacs-policy-test)#accounting auth-fail

rfs6000-37FABE(config-aaa-tacacs-policy-test)#accounting commands

rfs6000-37FABE(config-aaa-tacacs-policy-test)#accounting server preference
authorized-server-number

rfs6000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
 accounting auth-fail
 accounting commands
rfs6000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands

no	Resets values or disables commands

25.1.2 authentication

aaa-tacacs-policy

Configures user authentication parameters. Users are allowed or denied access to the network based on the authentication parameters set.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
authentication [access-method|directed-request|server|service]

authentication access-method [all|console|ssh|telnet|web] {(console|ssh|telnet|
web)}

authentication directed-request

authentication server <1-2> [host|retry-timeout-factor|timeout]

authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}

authentication server <1-2> retry-timeout-factor <50-200>

authentication server <1-2> timeout <3-60> {attempts <1-10>}

authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}
```

Parameters

- `authentication access-method [all|console|ssh|telnet|web] {(console|ssh|telnet)}`

access-method	Configures access modes for TACACS authentication. The options are: console, SSH, Telnet, Web, and all.
all	Authenticates users using all access modes (console, SSH, and Telnet)
console	Authenticates users using console access only
ssh	Authenticates users using SSH access only
telnet	Authenticates users using Telnet access only
web	Authenticates users using Web interface only

- `authentication directed-request`

directed-request	Enables user to specify TACACS server to use with `@server'. This option is disabled by default. The specified server should be present in the configured servers list.

- `authentication server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}`

server <1-2>	Configures a TACACS authentication server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.

host <IP/HOSTNAME>	Sets the TACACS server's IP address or hostname
secret [0 <SECRET>| 2 <SECRET>| <SECRET>]	Configures the secret key used to authenticate with the TACACS server • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the port used to connect to the TACACS server • <1-65535> – Specify a value for the TCP authentication port from 1 - 65535. The default port is 49.

- `authentication server <1-2> retry-timeout-factor <50-200>`

server <1-2>	Configures a TACACS authentication server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.
retry-timeout-factor <50-200>	Configures timeout scaling between two consecutive TACACS authentication retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.

- `authentication server <1-2> timeout <3-60> {attempts <1-10>}`

server <1-2>	Configures a TACACS authentication server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1- 2.
timeout <3-60>	Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted. • <3-60> – Specify a value from 3- 60 seconds. The default is 3 seconds.
attempts <1-10>	Optional. Indicates the number of retry attempts to make before giving up • <1-10> – Specify a value from 1 -10. The default is 3.

- `authentication service <SERVICE-NAME> {protocol <AUTHENTICATION-PROTO-NAME>}`

service <SERVICE-NAME>	Configures the TACACS authentication service name
protocol <AUTHENTICATION-PROTO-NAME>	Optional. Specify the authentication protocol used with this TACACS policy. A maximum of five entries is allowed.

Example

```
rfs6000-37FABE(config-aaa-tacacs-policy-test)#authentication directed-request

rfs6000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 accounting auth-fail
 accounting commands
rfs6000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands

no	Resets values or disables commands

25.1.3 authorization

aaa-tacacs-policy

Configures authorization parameters

This feature allows network administrators to limit user accessibility and configure varying levels of accessibility for different users.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
authorization [access-method|allow-privileged-commands|server]

authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}

authorization server [<1-2>|preference]

authorization server <1-2> [host|retry-timeout-factor|timeout]

authorizationserver <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|
<SECRET>]} {port <1-65535>}

authorization server <1-2> retry-timeout-factor <50-200>

authorization server <1-2> timeout <3-5> {attempts <1-3>}

authorization server preference [authenticated-server-host|authenticated-server-
number|none]
```

Parameters

- `authorization access-method [all|console|telnet|ssh] {(console|ssh|telnet)}`

access-method	Configures the access method for command authorization
all	Authorizes commands from all access methods
console	Authorizes commands from the console only
telnet	Authorizes commands from Telnet only
ssh	Authorizes commands from SSH only
{console|ssh|telnet}	Optional. Configures more than one access method for command authorization

- `authorization allow-privileged-commands`

allow-privileged-commands	Allows privileged commands execution without command authorization. This option is disabled by default.

- `authorization server <1-2> host <IP/HOSTNAME> {secret [0 <SECRET>|2 <SECRET>|<SECRET>]} {port <1-65535>}`

server <1-2>	Configures a TACACS authorization server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.

host <IP/HOSTNAME>	Sets the TACACS server's IP address or hostname
secret [0 <SECRET>| 2 <SECRET>|<SECRET>]	Optional. Configures the secret used to authorize with the TACACS server • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The shared key should not exceed 127 characters.
port <1-65535>	Optional. Specifies the port used to connect to the TACACS server • <1-65535> – Specify a value for the TCP authorization port from 1 - 65535. The default port is 49.

- `authorization server <1-2> retry-timeout-factor <50-200>`

server <1-2>	Configures a TACACS authorization server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server index from 1 - 2.
retry-timeout-factor <50-200>	Configures the scaling of timeouts between consecutive TACACS authorization retries • <50-200> – Specify the scaling factor from 50 - 200. The default is 100. A value of 100 indicates the interval between consecutive retires remains the same irrespective of the number of retries. A value lesser than 100 indicates the interval between consecutive retries reduces with each successive retry. A value greater than 100 indicates the interval between consecutive retries increases with each successive retry.

- `authorization server <1-2> timeout <3-5> {attempts <1-3>}`

server <1-2>	Configures a TACACS authorization server. Up to 2 TACACS servers can be configured • <1-2> – Specify the TACACS server's index from 1- 2.
timeout <3-5>	Configures the timeout, in seconds, for each request sent to the TACACS server. This is the time allowed to elapse before another request is sent to the TACACS server. If a response is received from the TACACS server within this time, no retry is attempted. • <3-5> – Specify a value from 3 - 5 seconds. The default is 3 seconds.
attempts <1-3>	Optional. Indicates the number of retry attempts to make before giving up • <1-3> – Specify a value from 1 - 3. The default is 3.

- `authorization server preference [authenticated-server-host|authenticated-server-number|none]`

preference	Configures the authorization server preference
authenticated-server-host	Sets the authentication server as the authorization server This parameter indicates the same server is used for authentication and authorization. The server is referred to by its hostname.

authenticated-server-number	Sets the authentication server as the authorization server This parameter indicates the same server is used for authentication and authorization. The server is referred to by its index or number.
none	Indicates the authorization server is independent of the authentication

Example

```
rfs6000-37FABE(config-aaa-tacacs-policy-test)#authorization allow-privileged-
commands

rfs6000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 authorization allow-privileged-commands
 accounting auth-fail
 accounting commands
rfs6000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands

no	Resets values or disables commands

25.1.4 no

aaa-tacacs-policy

Negates a AAA TACACS policy command or sets its default

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622,, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [accounting|authentication|authorization]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Provide the parameters needed to reset or disable the desired AAA-TACACS policy setting.

Example

The following example shows the AAA-TACACS policy 'test' settings before the 'no' commands are executed:

```
rfs6000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 authentication directed-request
 accounting server preference authorized-server-number
 authorization allow-privileged-commands
 accounting auth-fail
 accounting commands
rfs6000-37FABE(config-aaa-tacacs-policy-test)#

rfs6000-37FABE(config-aaa-tacacs-policy-test)#no authentication directed-request
rfs6000-37FABE(config-aaa-tacacs-policy-test)#no accounting auth-fail
rfs6000-37FABE(config-aaa-tacacs-policy-test)#no authorization allow-privileged-
commands
```

The following example shows the AAA-TACACS policy 'test' settings after the 'no' commands are executed:

```
rfs6000-37FABE(config-aaa-tacacs-policy-test)#show context
aaa-tacacs-policy test
 accounting server preference authorized-server-number
 accounting commands
rfs6000-37FABE(config-aaa-tacacs-policy-test)#
```

Related Commands

accounting	Configures TACACS accounting parameters
authentication	Configures TACACS authentication parameters
authorization	Configures TACACS authorization parameters

26 MESHPOINT

This chapter summarizes the Meshpoint commands in the CLI command structure.

Meshpoints are detector radios that monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

This chapter is organized as follows:

- *meshpoint-config-instance*
- *meshpoint-qos-policy-config-instance*
- *meshpoint-device-config-instance*

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

26.1 meshpoint-config-instance

MESHPOINT

MeshConnex (MCX) is a mesh networking technology that is comparable to the 802.11s mesh networking specification. MCX meshing uses a hybrid proactive/on-demand path selection protocol, similar to *Ad hoc On Demand Distance Vector* (AODV) routing protocols. This allows it to form efficient paths using multiple attachment points to a distribution WAN, or form purely ad-hoc peer-to-peer mesh networks in the absence of a WAN. Each device in the MCX mesh proactively manages its own path to the distribution WAN, but can also form peer-to-peer paths on demand to improve forwarding efficiency.

MCX is not compatible with MiNT Based meshing, though the two technologies can be enabled simultaneously in certain circumstances.

MCX is designed for large-scale, high-mobility outdoor mesh deployments. MCX continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MCX uses this data to dynamically form and continually maintain paths for forwarding network frames.

In MCX systems, a *meshpoint* (MP) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols will continually select the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID. The MeshID is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

Use the (config) instance to configure a meshpoint. To navigate to the meshpoint configuration instance, use the following command:

```
<DEVICE>(config)#meshpoint <MESHPOINT-NAME>

rfs6000-37FABE(config)#meshpoint test
rfs6000-37FABE(config-meshpoint-test)#?
Mesh Point Mode commands:
  allowed-vlans  Set the allowed VLANs
  beacon-format  The beacon format of this meshpoint
  control-vlan   VLAN for meshpoint control traffic
  data-rates     Specify the 802.11 rates to be supported on this meshpoint
  description    Configure a description of the usage of this meshpoint
  force          Force suboptimal paths
  meshid         Configure the Service Set Identifier for this meshpoint
  neighbor       Configure neighbor specific parameters
  no             Negate a command or set its defaults
  root           Set this meshpoint as root
  security-mode  The security mode of this meshpoint
  shutdown       Shutdown this meshpoint
  use            Set setting to use
  wpa2           Modify ccmp wpa2 related parameters

  clrscr         Clears the display screen
  commit         Commit all changes made in this session
  do             Run commands from Exec mode
  end            End current mode and change to EXEC mode
  exit           End current mode and down to previous mode
  help           Description of the interactive help system
  revert         Revert changes
  service        Service Commands
  show           Show running system information
```

```
  write          Write running configuration to memory or terminal

rfs6000-37FABE(config-meshpoint-test)#
```

The following table summarizes meshpoint configuration commands:

Table 26.1 *Meshpoint-Config commands*

Command	Description	Reference
allowed-vlans	Configures VLANs allowed on the meshpoint	*page 26-4*
beacon-format	Configures the beacon format for the meshpoint AP	*page 26-5*
control-vlan	Configures the VLAN where meshpoint control traffic traverses	*page 26-6*
data-rates	Configures the data rates supported per frequency band	*page 26-7*
description	Configures a human friendly description for this meshpoint	*page 26-11*
force	Forces formation of sub-optimal paths through the meshpoint's root node	*page 26-12*
meshid	Configures a unique ID for this meshpoint	*page 26-13*
neighbor	Configures the neighbor inactivity time out for this meshpoint	*page 26-14*
no	Negates a command or reverts settings to their default	*page 26-15*
root	Configures a meshpoint as the root meshpoint	*page 26-17*
security-mode	Configures the security mode on the meshpoint.	*page 26-19*
service	Allows only 802.11n capable neighbors to create a mesh connection	*page 26-20*
shutdown	Shuts down the meshpoint	*page 26-21*
use	Configures a QoS policy for use with this meshpoint	*page 26-22*
wpa2	Configures WPA2 encryption settings	*page 26-23*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

26.1.1 allowed-vlans

meshpoint-config-instance

Defines VLANs allowed to pass traffic on the mesh network. Use this command to add and remove VLANs from the list of allowed VLANs.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
allowed-vlans [<VLAN-ID>|add <VLAN-ID>|remove <VLAN-ID>]
```

Parameters

- `allowed-vlans [<VLAN-ID>|add <VLAN-ID>|remove <VLAN-ID>]`

allowed-vlans	Defines VLANs allowed access on the mesh network
<VLAN-ID>	The VLAN ID or the range of IDs to be managed. A single VLAN or multiple VLANs can be added to the list of allowed VLANs. When adding multiple VLANs, specify the range (for example, 10-20, 25, 30-35). Use this command to create a VLAN list on a new meshpoint.
add <VLAN-ID>	Adds a single VLAN or a range of VLANs to the list of allowed VLANs. To specify a range of VLANs, specify the first and last VLAN ID in the range separated by a hyphen (for example, 1-10). • <VLAN-ID> – Specify the VLAN ID or the range of IDs to add.
remove <VLAN-ID>	Removes a single VLAN or a range of VLANs from the list of allowed VLANs • <VLAN-ID> – Specify the VLAN ID or the range of IDs to remove.

Example

```
rfs6000-37FABE(config-meshpoint-test)#allowed-vlans 1

rfs6000-37FABE(config-meshpoint-test)#allowed-vlans add 10-23

rfs6000-37FABE(config-meshpoint-test)#allowed-vlans remove 17

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Clears the list of VLANs allowed access to the mesh network

26.1.2 beacon-format

meshpoint-config-instance

Configures the beacon transmission format for this meshpoint. Beacons are transmitted periodically to advertise that a wireless network is available. It contains all the required information for a device to connect to the network.

The beacon format advertises how a mesh capable AP7161 acts. APs can act either as an access point or a meshpoint.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
beacon-format [access-point|mesh-point]
```

Parameters

- `beacon-format [access-point|mesh-point]`

beacon-format	Configures how a mesh capable AP71XX acts in a mesh network
access-point	Uses access point style beacons
mesh-point	Uses meshpoint style beacons (this is the default setting)

Example

```
rfs6000-37FABE(config-meshpoint-test)#beacon-format mesh-point

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Resets the beacon format for this meshpoint to its default (mesh-point)

26.1.3 control-vlan

meshpoint-config-instance

Configures a VLAN as the dedicated control VLAN

Mesh management traffic can be sent over a dedicated VLAN. This dedicated VLAN is known as the control VLAN, and should be configured in the backhaul port of all the access points configured as meshpont roots. Once configured, the control VLAN enables communication between meshpoint's root APs.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]
```

Parameters

- `control-vlan [<1-4094>|<VLAN-ALIAS-NAME>]`

control-vlan	Configures a VLAN as a dedicated carrier of mesh management traffic
[<1-4094>| <VLAN-ALIAS-NAME>]	Configures the control VLAN • <1-4094> – Specify the control VLAN from 1 - 4094. The default is VLAN 1. • <VLAN-ALIAS-NAME> – Uses a vlan-alias to specify the control vlan. If using a vlan-alias, ensure that it is existing and configured. If VLAN 1 is configured as the control VLAN, ensure that the VLAN is configured in the wired port of all access points belonging to same meshpoint. **Note:** Control VLAN need not necessarily be added in the allowed VLAN list.

Example

```
rfs6000-37FABE(config-meshpoint-test)#control-vlan 1

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Resets the control VLAN for this meshpoint to its default of 1

26.1.4 data-rates

meshpoint-config-instance

Configures individual data rates for the 2.4 GHz and 5.0 GHz frequency bands. In Mesh network, a mesh point is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 mesh points can be created and 2 can be created per radio. Each mesh point radio can have carefully administrated radio rates specific to the 2.4 or 5 GHz band. Use this command to configure these radio rates.

NOTE: Ensure that the basic data rates configured on a meshpoint's root and non-root access points is the same.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
data-rates [2.4GHz|5GHz]

data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]

data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|
basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|
basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)

data-rates 5GHz [a-only|an|default]

data-rates 5GHz custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-
18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-
15|mcs0-7|mcs8-15|basic-mcs0-7)
```

Parameters

- `data-rates 2.4GHz [b-only|bg|bgn|default|g-only|gn]`

data-rates 2.4GHz	Configures preset data rates for the 2.4 GHz frequency.
b-only	Configures data rate for the meshpoint using 802.11b only rates.
bg	Configures data rate for the meshpoint using 802.11b and 802.11g rates.
default	Configures data rate for the meshpoint at a pre-configured default rate for this frequency.
g-only	Configures data rate for the meshpoint using 802.11g only rates.
gn	Configures data rate for the meshpoint using 802.11g and 802.11n rates.

- `data-rates 2.4GHz custom (1|11|12|18|2|24|36|48|5.5|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)`

data-rates 2.4GHz	Configures the preset data rates for the 2.4 GHz frequency Define both minimum *Basic* and optimal *Supported* rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band. Contd..

	These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a supported MCS index.Set a *Modulation and Coding Scheme* (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Meshpoints can communicate as long as they support the same basic MCS (as well as non-802.11n basic rates). The selected rates apply to associated client traffic within this mesh point only.
custom (1|11|12|18|2|24|36| 48|5.5|54|6|9| basic-1|basic-11| basic-12|basic-18| basic-2|basic-24| basic-36|basic-48| basic-5.5|basic-54| basic-6|basic-9| mcs0-15|mcs0-7| mcs8-15| basic-mcs0-7)	Configures custom rates • 1 – Configures the available rate at 1 Mbps • 2 – Configures the available rate at 2 Mbps • 5.5 – Configures the available rate at 5.5 Mbps • 6 – Configures the available rate at 6 Mbps • 9 – Configures the available rate at 9 Mbps • 11 – Configures the available rate at 11 Mbps • 12 – Configures the available rate at 12 Mbps • 18 – Configures the available rate at 18 Mbps • 24 – Configures the available rate at 24 Mbps • 36 – Configures the available rate at 36 Mbps • 48 – Configures the available rate at 48 Mbps • 54 – Configures the available rate at 54 Mbps • basic-1 – Configures the available rate at a basic rate of 1 Mbps • basic-2 – Configures the available rate at a basic rate of 2 Mbps • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps • basic-6 – Configures the available rate at a basic rate of 6 Mbps • basic-9 – Configures the available rate at a basic rate of 9 Mbps • basic-11 – Configures the available rate at a basic rate of 11 Mbps • basic-12 – Configures the available rate at a basic rate of 12 Mbps • basic-18 – Configures the available rate at a basic rate of 18 Mbps • basic-24 – Configures the available rate at a basic rate of 24 Mbps • basic-36 – Configures the available rate at a basic rate of 36 Mbps • basic-48 – Configures the available rate at a basic rate of 48 Mbps • basic-54 – Configures the available rate at a basic rate of 54 Mbps • basic-mcs0-7 – Configures the MCS index range of 0 - 7 for basic rate • mcs0-7 – Configures the MCS index range of 0-7 as the data rate • mcs0-15 – Configures the MCS index range of 0-15 as the data rate • msc8-15 – Configures the MCS index range of 8-15 as the data rate Multiple choices can be made from the above list of rates.

- `data-rates 5GHz [a-only|an|default]`

data-rates 5GHz	Configures the preset data rates for the 5.0 GHz frequency
a-only	Configures the data rate for the meshpoint using 802.11a only rates
bn	Configures the data rate for the meshpoint using 802.11a and 802.11n rates

default	Configures the data rate for the meshpoint at a pre-configured default rate for this frequency
g-only	Configures the data rate for the meshpoint using 802.11g only rates
gn	Configures the data rate for the meshpoint using 802.11g and 802.11n rates

```
• data-rates 5GHz custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|
basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|
mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)
```

data-rates 5GHz	Configures the preset data rates for the 5.0 GHz frequency Define both minimum Basic and optimal Supported rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a supported MCS index. Set a MCS in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-802.11n basic rates). The selected rates apply to associated client traffic within this mesh point only.
custom (12|18|24|36|48|54|6|9|basic-1|basic-11|basic-12|basic-18|basic-2|basic-24|basic-36|basic-48|basic-5.5|basic-54|basic-6|basic-9|mcs0-15|mcs0-7|mcs8-15|basic-mcs0-7)	Configures custom rates • 6 – Configures the available rate at 6 Mbps • 9 – Configures the available rate at 9 Mbps • 12 – Configures the available rate at 12 Mbps • 18 – Configures the available rate at 18 Mbps • 24 – Configures the available rate at 24 Mbps • 36 – Configures the available rate at 36 Mbps • 48 – Configures the available rate at 48 Mbps • 54 – Configures the available rate at 54 Mbps • basic-1 – Configures the available rate at a basic rate of 1 Mbps • basic-2 – Configures the available rate at a basic rate of 2 Mbps • basic-5.5 – Configures the available rate at a basic rate of 5.5 Mbps • basic-6 – Configures the available rate at a basic rate of 6 Mbps • basic-9 – Configures the available rate at a basic rate of 9 Mbps • basic-11 – Configures the available rate at a basic rate of 11 Mbps • basic-12 – Configures the available rate at a basic rate of 12 Mbps • basic-18 – Configures the available rate at a basic rate of 18 Mbps • basic-24 – Configures the available rate at a basic rate of 24 Mbps • basic-36 – Configures the available rate at a basic rate of 36 Mbps • basic-48 – Configures the available rate at a basic rate of 48 Mbps • basic-54 – Configures the available rate at a basic rate of 54 Mbps Cotnd..

	• basic-mcs0-7 – Configures the MCS index range of 0-7 for basic rate • mcs0-7 – Configures the MCS index range of 0-7 as the data rate • mcs0-15 – Configures the MCS index range of 0-15 as the data rate • msc8-15 – Configures the MCS index range of 8-15 as the data rate Multiple choices can be made from the above list of rates.

Example

```
rfs6000-37FABE(config-meshpoint-test)#data-rates 2.4GHz bgn

rfs6000-37FABE(config-meshpoint-test)#data-rates 5GHz an

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Resets data rates for each frequency band for this meshpoint

26.1.5 description

meshpoint-config-instance

Configures a brief description for this meshpoint. Use this command to describe this meshpoint and its features.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
description <DESCRIPTION>
```

Parameters

- `description <DESCRIPTION>`

description	Configures a description for this meshpoint
<DESCRIPTION>	The text describing this meshpoint

Example

```
rfs6000-37FABE(config-meshpoint-test)#description "This is an example of a
meshpoint description"

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid test
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Removes the human friendly description provided for this meshpoint

26.1.6 force

meshpoint-config-instance

Forces formation of sub-optimal paths through the meshpoint's root node. As per legacy behavior, non-root devices under the same root, communicated by forming direct paths through the network. This option allows
non-root devices, within the meshpoint, to communicate by forming paths through the root node.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
force peer-paths-through-root
```

Parameters

- `force peer-paths-through-root`

force	Enables formation of sub-optimal paths through the meshpoint root node. This option is disabled by default
peer-paths-through-root	Enables non-root devices to communicate by forming sub-optimal paths through the root node

Example

```
nx9500-6C8809(config-meshpoint-test)#force peer-paths-through-root

nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode none
 no root
 force peer-paths-through-root
nx9500-6C8809(config-meshpoint-test)#
```

Related Commands

no	Disables formation of sub-optimal paths through the meshpoint's root node

26.1.7 meshid

meshpoint-config-instance

Configures a unique *Service Set Identifier* (SSID) for this meshpoint. This ID is used to uniquely identify this meshpoint.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
meshid <MESH-SSID>
```

Parameters

- `meshid <MESH-SSID>`

meshid	Configures a unique SSID for the meshpoint
<MESH-SSID>	The unique SSID configured for this meshpoint **Note:** The mesh SSID is case sensitive and should not exceed 32 characters.

Example

```
rfs6000-37FABE(config-meshpoint-test)#meshid TestingMeshPoint

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Removes the SSID configured for this meshpoint

26.1.8 neighbor

meshpoint-config-instance

This command configures the inactivity time out value for neighboring devices. If a frame is not received from the neighbor device for the configured time, then client resources are removed.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
neighbor inactivity-timeout <60-86400>
```

Parameters

- `neighbor inactivity-timeout <60-86400>`

neighbor inactivity-timeout <60-86400>	Configures the neighbor inactivity timeout in seconds. This represents the allowed interval between frames received from a neighbor before their client privileges are revoked. • <60-86400> – Specify a value from 60 - 86400 seconds. The default is 120 seconds.

Example

```
rfs6000-37FABE(config-meshpoint-test)#neighbor inactivity-timeout 300

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 no root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Removes the configured neighbor inactivity time out value for this meshpoint

26.1.9 no

meshpoint-config-instance

Negates meshpoint commands or resets their values to default

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [allowed-vlans|beacon-format|control-vlan|description|force|meshid|root|
security-mode|shutdown]

no data-rates [2.4GHz|5GHz]
no force peer-paths-through-root
no neighbor inactivity-timeout
no use [aaa-policy|meshpoint-qos-policy]

no wpa2 [eap|key-rotation|psk]
no wpa2 eap [auth-type|identity|peap-mschapv2|tls trustpoint]
no wpa2 key-rotation [broadcast|unicast]
no wpa2 psk

no service allow-ht-only
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts this meshpoint settings to default based on the parameters passed

Example

```
rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
rfs6000-37FABE(config-meshpoint-test)#

rfs6000-37FABE(config-meshpoint-test)#no allowed-vlans
rfs6000-37FABE(config-meshpoint-test)#no beacon-format
rfs6000-37FABE(config-meshpoint-test)#no control-vlan
rfs6000-37FABE(config-meshpoint-test)#no description
rfs6000-37FABE(config-meshpoint-test)#no meshid
rfs6000-37FABE(config-meshpoint-test)#no root
rfs6000-37FABE(config-meshpoint-test)#no security-mode
```

```
rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 beacon-format mesh-point
 control-vlan 1
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode none
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 no root

rfs6000-37FABE(config-meshpoint-test)#no data-rates 2.4GHz
rfs6000-37FABE(config-meshpoint-test)#no data-rates 5GHz

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 beacon-format mesh-point
 control-vlan 1
 neighbor inactivity-timeout 300
 security-mode none
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 no root
rfs6000-37FABE(config-meshpoint-test)#

nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode none
 no root
 force peer-paths-through-root
nx9500-6C8809(config-meshpoint-test)#

nx9500-6C8809(config-meshpoint-test)#no force peer-paths-through-root

nx9500-6C8809(config-meshpoint-test)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode none
 no root
nx9500-6C8809(config-meshpoint-test)#
```

26.1.10 root

meshpoint-config-instance

Configures this meshpoint as the root meshpoint. Root meshpoints are generally tied to an Ethernet backhaul for wired connectivity. By default this option is disabled.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
root
```

Parameters

None

Example

There are two ways of configuring root access points within a meshpoint.

1 First method:

- Configure two meshpoints, having the *same meshid*, one with the *root* option enabled and the other configured as *no root*:
- Apply the root meshpoint to the *root* access point and the *no-root* meshpoint to the *non-root* access points.

The following examples show the configuration of a meshpoint for the *root* access point:

```
rfs6000-37FABE(config)#meshpoint root
rfs6000-37FABE(config-meshpoint-root)#

rfs6000-37FABE(config-meshpoint-root)#meshid test
rfs6000-37FABE(config-meshpoint-root)#root
rfs6000-37FABE(config-meshpoint-root)#security-mode eap
rfs6000-37FABE(config-meshpoint-root)#commit

rfs6000-37FABE(config-meshpoint-root)#show context
meshpoint test-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 root
rfs6000-37FABE(config-meshpoint-root)#
```

The following examples show the configuration of a meshpoint for *non-root* access points:

```
rfs6000-37FABE(config)#meshpoint no-root
rfs6000-37FABE(config-meshpoint-no-root)#

rfs6000-37FABE(config-meshpoint-no-root)#meshid test
rfs6000-37FABE(config-meshpoint-no-root)#security-mode eap

rfs6000-37FABE(config-meshpoint-no-root)#show context
meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 no root
rfs6000-37FABE(config-meshpoint-no-root)#
```

2 Second method:

- Configure a *no-root* meshpoint and apply to all access points in the meshpoint.
- Log into the *meshpoint-device > no-root* configuration mode of the *root* access point and *enable root*.

```
rfs6000-37FABE(config-meshpoint-no-root)#show context
meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 no root
rfs6000-37FABE(config-meshpoint-no-root)#

rfs6000-37FABE(config)#ap81xx B4-C7-99-71-17-28

rfs6000-37FABE(config-device-B4-C7-99-71-17-28)#meshpoint-device no-root
rfs6000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#

rfs6000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#show context
 meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 no root
rfs6000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#

rfs6000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#root

rfs6000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#show context
 meshpoint no-root
 meshid test
 beacon-format mesh-point
 control-vlan 1
 security-mode eap
 root
rfs6000-37FABE(config-device-B4-C7-99-71-17-28-meshpoint-no-root)#
```

Related Commands

no	Removes the configuration of this meshpoint as a root meshpoint

26.1.11 security-mode

meshpoint-config-instance

Configures the security mode for this meshpoint

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
security-mode [eap|none|psk]
```

Parameters

- `security-mode [eap|none|psk]`

security-mode	Configures the security mode for this meshpoint
eap	Uses 802.1X/EAP as the security mode. When using this option, use the *wpa2* command to specify the EAP authentication type and related parameters.
none	No security is configured for this meshpoint
psk	Uses *Pre Shared Key* (PSK) as the security mode. When using this option, use the *wpa2* command to enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point.

Example

The following example shows *root meshpoint* configuration with PSK authentication enabled:

```
rfs6000-37FABE(config-meshpoint-test)#security-mode psk

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 root
rfs6000-37FABE(config-meshpoint-test)#
```

The following example shows *root meshpoint* configuration with EAP authentication enabled:

```
rfs6000-37FABE(config-meshpoint-root)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 101
 allowed-vlans 101,103
 use aaa-policy test
 security-mode eap
 root
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Resets the security configuration for this meshpoint to “none”. This indicates that no security is configured for this meshpoint.

26.1.12 service

meshpoint-config-instance

Use this command to allow only those neighbors who are capable of 802.11n data rates to associate with this meshpoint.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
service [allow-ht-only|show cli]
```

Parameters

```
• service [allow-ht-only|show cli]
```

service allow-ht-only	Allows only those neighbors who are capable of high throughput data rates (802.11n data rates) to associate with the meshpoint
service show cli	Displays running system configuration

Example

```
rfs6000-37FABE(config-meshpoint-test)#service allow-ht-only

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
 service allow-ht-only
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Removes the restriction that only 802.11n capable neighbor devices can associate with this meshpoint
service	Invokes service commands to troubleshoot or debug

26.1.13 shutdown

meshpoint-config-instance

Shuts down this meshpoint. Use this command to prevent an AP from participating in a mesh network.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
shutdown
```

Parameters

None

Example

```
rfs6000-37FABE(config-meshpoint-test)#shutdown
rfs6000-37FABE(config)
```

Related Commands

no	Enables an AP as a meshpoint

26.1.14 use

meshpoint-config-instance

Uses a *Quality of Service* (QoS) policy defined specifically for meshpoints. To use this QoS policy, it must be defined. To define a meshpoint QoS policy, see *meshpoint-qos-policy-config-instance*.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use [aaa-policy <AAA-POLICY-NAME>|meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>]
```

Parameters

```
• use [aaa-policy <AAA-POLICY-NAME>|meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>]
```

use meshpoint-qos-policy <MESHPOINT-QOS-POLICY-NAME>	Configures this meshpoint to use a predefined meshpoint QoS policy • <MESHPOINT-QOS-POLICY-NAME> – Specify the meshpoint QoS policy name (should be existing and configured).
use aaa-policy <AAA-POLICY-NAME>	Configures this meshpoint to use a predefined aaa-policy • <AAA-POLICY-NAME> – Specify the aaa-policy name (should be existing and configured).

Example

```
rfs6000-37FABE(config-meshpoint-test)#use meshpoint-qos-policy test

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 root
 use meshpoint-qos-policy test
rfs6000-37FABE(config-meshpoint-test)#
```

Related Commands

no	Removes the meshpoint QoS policy associated with this meshpoint
meshpoint-qos-policy-config-instance	Creates and configures a meshpoint QoS policy

26.1.15 wpa2

meshpoint-config-instance

Use this command to configure the parameters of authentication mode specified using the 'security-mode' keyword. This command also allows you to set a unicast and broadcast key rotation interval.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
wpa2 [eap|psk|key-rotation]

wpa2 key-rotation [broadcast|unicast] <30-86400>

wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]

wpa2 eap [auth-type|identity|peap-mschapv2|tls]

wpa2 eap [auth-type [peap-mschapv2|tls]|identity <WORD>]

wpa2 eap peap-mschapv2 user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>]
{trustpoint <TRUSTPOINT-NAME>}

wpa2 eap tls trustpoint <TRUSTPOINT-NAME>
```

Parameters

- `wpa2 key-rotation [broadcast|unicast] <30-86400>`

wpa2 key-rotation	Enables periodic rotation of encryption keys used for broadcast and unicast traffic
broadcast	Configures key rotation interval for broadcast and multicast traffic. This option is disabled by default. When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Key rotation enhances the broadcast traffic security on the WLAN.
unicast	Configures key rotation interval for unicast traffic. This option is disabled by default.
<30-86400>	Configures key rotation interval from 30 - 86400 seconds for unicast or broadcast transmission

- `wpa2 psk [0 <SECRET>|2 <SECRET>|<SECRET>]`

wpa2 psk	Configures the shared key for authentication mode PSK. If the security mode is set as 'psk' using the 'security-mode' keyword, use this command to configure the pre-shared key.
secret [0 <SECRET>| 2 <SECRET>|<SECRET>]	Configures the PSK used to authenticate this meshpoint with other meshpoints in the network • 0 <SECRET> – Configures a clear text secret • 2 <SECRET> – Configures an encrypted secret • <SECRET> – Specify the secret key. The pre-shared key can be in ASCII (8 to 63 characters in length) or Hexadecimal (not exceeding 64 characters in length) formats.

- `wpa2 eap [auth-type [peap-mschapv2|tls]|identity <WORD>]`

wpa2 eap	Configures the 802.1X/EAP based authentication type for this meshpoint. If the security mode is set as 'eap' using the 'security-mode' keyword, use this command to specify the EAP type. The options are: peap-mschapv2 and tls.
auth-type [peap-mschapv2|tls]	Specifies the EAP authentication type. The options are: • peap-mschapv2 – Configures EAP authentication type as *Protected Extensible Authentication Protocol* (PEAP) with default auth type MSCHAPv2. This is the default setting. If using auth-type as 'peap-mschapv2', use the 'peap-mschapv2' keyword to configure user credentials and trustpoint details. • tls – Configures EAP authentication type as *Transport Layer Security* (TLS) If using auth-type as 'tls', use the 'tls' keyword to configure trustpoint details. **Note:** The certificate should be issued from an Enterprise or public certificate authority to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials.
identity <WORD>	Configures identity to be used during phase1 authentication • <WORD> – Enter a string up to 256 characters in length (this should not be actual identity of user but some anonymous/bogus username)

- `wpa2 eap peap-mschapv2 user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>] {trustpoint <TRUSTPOINT-NAME>}`

wpa2 eap peap-mschapv2	Configures PEAP-related user credentials and trustpoint details
user <USER-NAME> password [0 <WORD>|2 <WORD>|<WORD>]	Specify the user credentials used for authentication • user <USER-NAME> – Specify the user name. • password [0 <WORD>|2 <WORD>|<WORD>] – Specify the password associated with the specified user.
trustpoint <TRUSTPOINT-NAME>	Optional. Associates a trustpoint used for installing CA certificate and verifying server certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be existing and configured).

- `wpa2 eap tls trustpoint <TRUSTPOINT-NAME>`

wpa2 eap tls	Configures TLS client related parameters
trustpoint <TRUSTPOINT-NAME>	Configures trustpoint details • trustpoint <TRUSTPOINT-NAME> – Assigns a trustpoint to be used for installing TLS client certificate, client private key, and CA certificate • <TRUSTPOINT-NAME> – Specify the trustpoint name (should be existing and configured)

Example

```
rfs6000-37FABE(config-meshpoint-test)#wpa2 key-rotation broadcast 600
rfs6000-37FABE(config-meshpoint-test)#wpa2 key-rotation unicast 1200
rfs6000-37FABE(config-meshpoint-test)#wpa2 psk Test Company

rfs6000-37FABE(config-meshpoint-test)#show context
meshpoint test
 description "This is an example of a meshpoint description"
 meshid TestingMeshPoint
```

```
 shutdown
 beacon-format mesh-point
 control-vlan 1
 allowed-vlans 1,10-16,18-23
 neighbor inactivity-timeout 300
 data-rates 2.4GHz bgn
 data-rates 5GHz an
 security-mode psk
 wpa2 psk 0 Test Company
 wpa2 key-rotation unicast 1200
 wpa2 key-rotation broadcast 600
 root
rfs6000-37FABE(config-meshpoint-test)#
```

The following example shows *root meshpoint* configuration with EAP authentication enabled:

```
rfs6000-37FABE(config-meshpoint-root)#show context
meshpoint test
 meshid test
 beacon-format mesh-point
 control-vlan 101
 allowed-vlans 101,103
 use aaa-policy test
 security-mode eap
 root
rfs6000-37FABE(config-meshpoint-test)#
```

The following example shows *non-root meshpoint* configuration with *EAP PEAP-MSCHAPv2* authentication:

```
rfs6000-37FABE(config-meshpoint-testNoRoot)#show context
meshpoint testNoRoot
 meshid test
 beacon-format mesh-point
 control-vlan 101
 allowed-vlans 101,103
 security-mode eap
 wpa2 eap peap-mschapv2 user tester123 password 0 testing1234 trustpoint mesh1
 wpa2 eap identity tester123
 no root
rfs6000-37FABE(config-meshpoint-testNoRoot)#
```

The following example shows *non-root meshpoint* configuration with *EAP TLS* authentication:

```
rfs6000-37FABE(config-meshpoint-testNoRoot)#show context
meshpoint testNoRoot
 meshid test
 beacon-format mesh-point
 control-vlan 101
 allowed-vlans 101,103
 security-mode eap
 wpa2 eap peap-mschapv2 user tester123 password 0 testing1234 trustpoint mesh1
 wpa2 eap tls trustpoint mesh1
 wpa2 eap identity tester123
 no root
rfs6000-37FABE(config-meshpoint-testNoRoot)#
```

Related Commands

no	Resets PSK configuration and key rotation duration

26.2 meshpoint-qos-policy-config-instance

MESHPOINT

Mesh QoS provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS helps ensure each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as video, voice and data.packets within each category are processed based on the weights defined for each mesh point.

To create a meshpoint, see *meshpoint-config-instance*. A meshpoint QoS policy is created from the (config) instance. To create a meshpoint QoS policy use the following command:

```
<DEVICE>(config)#meshpoint-qos-policy <POLICYNAME>

rfs6000-37FABE(config)#meshpoint-qos-policy test
rfs6000-37FABE(config-meshpoint-qos-test)#

rfs6000-37FABE(config-meshpoint-qos-test)#?
Mesh Point QoS Mode commands:
  accelerated-multicast  Configure accelerated multicast streams address and
                         forwarding QoS classification
  no                     Negate a command or set its defaults
  rate-limit             Configure traffic rate-limiting parameters on a
                         per-meshpoint/per-neighbor basis

  clrscr                 Clears the display screen
  commit                 Commit all changes made in this session
  do                     Run commands from Exec mode
  end                    End current mode and change to EXEC mode
  exit                   End current mode and down to previous mode
  help                   Description of the interactive help system
  revert                 Revert changes
  service                Service Commands
  show                   Show running system information
  write                  Write running configuration to memory or terminal

rfs6000-37FABE(config-meshpoint-qos-test)#
```

The following table summarizes the meshpoint-qos-policy configuration commands:

Table 26.2 *Meshpoint-QoS-Policy Config Commands*

Command	Description	Reference
accelerated-multicast	Configures accelerated multicast parameters	*page 26-27*
no	Negates a command or reverts settings to their default	*page 26-29*
rate-limit	Configures the rate limits for this QoS policy	*page 26-30*

26.2.1 accelerated-multicast

meshpoint-qos-policy-config-instance

Configures the accelerated multicast stream's address and forwarding QoS classification

NOTE: For accelerated multicast feature to work, IGMP querier must be enabled.

When a user joins a multicast stream, an entry is created in the device's (AP or wireless controller) snoop table and the entry is set to expire after a set time period. Multicast packets are forwarded to the appropriate wireless LAN or mesh until this entry is available in the snoop table.

Snoop querier keeps the snoop table current by updating entries that are set to expire. It also keeps an entry for each multicast stream till there are users registered for the stream.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
accelerated-multicast [<MULTICAST-IP>|autodetect] {classification [background|
best-effort|trust|video|voice]}
```

Parameters

```
• accelerated-multicast [<MULTICAST-IP>|autodetect] {classification
[background|best-effort|trust|video|voice]}
```

accelerated-multicast	Configures the accelerated multicast stream address and forwarding QoS classification
<MULTICAST-IP>	Specify a list of multicast addresses and classifications. Packets are accelerated when the destination address matches.
autodetect	Lets the system to automatically detect multicast streams to be accelerated This option allows the administrator to convert multicast packets to unicast in order to provide better overall airtime utilization and performance. The system can be configured to automatically detect multicast streams and convert them to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, there are a number of classification mechanisms applied to the stream and the administrator can select what type of classification they would want. Classification types are trust, voice, video, best effort, and background.
classification	Optional. Defines the QoS classification to apply to a multicast stream. The following options are available: • background • best effort • trust • video • voice

Example

```
rfs6000-37FABE(config-meshpoint-qos-test)#accelerated-multicast 224.0.0.1
classification video

rfs6000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 accelerated-multicast 224.0.0.1 classification video
rfs6000-37FABE(config-meshpoint-qos-test)#
```

Related Commands

no	Resets accelerated multicast configurations for this meshpoint QoS policy

26.2.2 no

meshpoint-qos-policy-config-instance

Negates the commands for meshpoint QoS policy or resets their values to their default

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [accelerated-multicast|rate-limit]

no accelerated-multicast [<MULTICAST-IP>|autodetect]
no rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size|rate}
no rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background|
   best-effort|video|voice]}
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts this meshpoint QoS policy settings to default based on the parameters passed

Example

```
rfs6000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air rate 80000
 rate-limit meshpoint from-air red-threshold video 80
 rate-limit meshpoint from-air red-threshold voice 70
 accelerated-multicast 224.0.0.1 classification video

rfs6000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air rate
rfs6000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-
threshold video 80
rfs6000-37FABE(config-meshpoint-qos-test)#no rate-limit meshpoint from-air red-
threshold voice 70

rfs6000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 accelerated-multicast 224.0.0.1 classification video
rfs6000-37FABE(config-meshpoint-qos-test)#
```

26.2.3 rate-limit

meshpoint-qos-policy-config-instance

Configures the rate limiting of traffic on a per meshpoint or per neighbor basis

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic, bombardments and interference are caused by numerous sources, such as network loops, faulty devices, or malicious software (such as a worm or virus) that has infected one or more branch-level devices. Rate limiting limits the maximum rate sent to or received from the wireless network (and meshpoint) per neighbor. It prevents any single user from overwhelming the wireless network. It also provides differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the network and data transmitted from a mesh point's neighbor.

Before defining rate limit thresholds for meshpoint transmit and receive traffic, it is recommended that you define the normal number of ARP, broadcast, multicast, and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX
- Wireless Controllers — RFS6000
- Service Platforms — NX6524, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
rate-limit [meshpoint|neighbor]

rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000>}

rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}
```

Parameters

```
• rate-limit [meshpoint|neighbor] [from-air|to-air] {max-burst-size <2-1024>|rate <50-1000000>}
```

meshpoint	Configures rate limit parameters for all data received from any meshpoint in the mesh network. This option is disabled by default.
neighbor	Configures rate limit parameters for neighboring meshpoint devices. Enables rate limiting for data transmitted from the client to its associated access point radio and connected controller. This option is disabled by default.
from-air	Configures rate limits for traffic from the wireless neighbor to the network.
to-air	Configures rate limits for traffic from the network to the wireless neighbor.

max-burst-size <2-1024>	Optional. Configures the maximum burst size in kilobytes. • <2-1024> – Set a value from 2 - 1024 kbytes. For a meshpoint: The smaller the burst, the less likely that the transmit packet transmission results in congestion for the meshpoint's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320 kbytes. For a neighbor: The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.
rate <50-1000000>	Optional. Defines a receive or transmit rate limit in kilobytes per second • <50-1000000> – Set a value from 50 - 1000000 kbps. For a meshpoint: This limit constitutes a threshold for the maximum number of packets transmitted or received over the meshpoint (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps. For a neighbor: This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.

• `rate-limit [meshpoint|neighbor] [from-air|to-air] {red-threshold [background <0-100>|best-effort <0-100>|video <0-100>|voice <0-100>]}`

meshpoint	Configures rate limit parameters for a meshpoint
neighbor	Configures rate limit parameters for neighboring meshpoint devices
from-air	Configures rate limits for traffic from the wireless neighbor to the network
to-air	Configures rate limit value for traffic from the network to the wireless neighbor
red-threshold	Optional. Configures *random early detection* threshold (RED threshold) for traffic class
background <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • background <0-100> – Configures the threshold for low priority (background) traffic • <0-100> – Specify a value from 0 - 100. For a meshpoint: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. For a neighbor: This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.

best-effort <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • best-effort <0-100> – Configures the threshold for best effort traffic • <0-100> – Specify a value from 0 - 100. For a meshpoint: This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%. For a neighbor: This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
video <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • video <0-100> – Configures the threshold for video traffic • <0-100> – Specify a value from 0 - 100. For a meshpoint: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%. For a neighbor: This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.
voice <0-100>	The following keyword is applicable to the 'from-air' and 'to-air' traffics. • voice <0-100> – Configures the threshold for voice traffic • <0-100> – Specify a value from 0 - 100. For a meshpoint: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. For a neighbor: This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0% and implies no early random drops will occur.

Example

```
rfs6000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air max-
burst-size 800

rfs6000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air max-burst-size 800
 accelerated-multicast 224.0.0.1 classification video

rfs6000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air rate
80000

rfs6000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-
threshold video 80

rfs6000-37FABE(config-meshpoint-qos-test)#rate-limit meshpoint from-air red-
threshold voice 70
```

```
rfs6000-37FABE(config-meshpoint-qos-test)#show context
meshpoint-qos-policy test
 rate-limit meshpoint from-air rate 80000
 rate-limit meshpoint from-air max-burst-size 800
 rate-limit meshpoint from-air red-threshold video 80
 rate-limit meshpoint from-air red-threshold voice 70
 accelerated-multicast 224.0.0.1 classification video
rfs6000-37FABE(config-meshpoint-qos-test)#
```

Related Commands

no	Resets traffic rate limit settings for this meshpoint QoS policy

26.3 meshpoint-device-config-instance

MESHPOINT

The following table lists the meshpoint device configuration commands:

Table 26.3 *Other meshpoint-related commands*

Command	Description	Reference
meshpoint-device	Configures an access point as a meshpoint device and enters its configuration mode	*page 26-35*
meshpoint-device-commands	Invokes the meshpoint-device configuration commands	*page 26-37*

26.3.1 meshpoint-device

meshpoint-device-config-instance

This command configures an access point to use a defined meshpoint. To configure this feature use one of the following options:

- navigate to the device profile config context (used when configuring access point profile on a controller)
- navigate to the device's config context using the self command (used when configuring a logged on access point)

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
meshpoint-device <MESHPOINT-NAME>
```

Parameters

- `meshpoint-device <MESHPOINT-NAME>`

meshpoint-device	Configures the AP as a meshpoint device and sets its parameters
<MESHPOINT-NAME>	The meshpoint to configure the AP with (should be existing and configured)

Example

```
rfs6000-37FABE(config)#profile ap71xx AP71XXTestProfile
rfs6000-37FABE(config-profile-AP71XXTestProfile)#meshpoint-device test
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#?
Mesh Point Device Mode commands:
  Mesh Point Device Mode commands:
  acs           Configure auto channel selection parameters
  exclude       Exclude neighboring Mesh Devices
  hysteresis    Configure path selection SNR hysteresis values
  monitor       Event Monitoring
  no            Negate a command or set its defaults
  path-method   Path selection method used to find a root node
  preferred     Configure preferred path parameters
  root          Set this meshpoint as root
  root-select   Root selection method parameters

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#meshpoint-device
test
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#?
Mesh Point Device Mode commands:
  acs           Configure auto channel selection parameters
  exclude       Exclude neighboring Mesh Devices
  hysteresis    Configure path selection SNR hysteresis values
  monitor       Event Monitoring
  no            Negate a command or set its defaults
  path-method   Path selection method used to find a root node
  preferred     Configure preferred path parameters
  root          Set this meshpoint as root
  root-select   Root selection method parameters

  clrscr        Clears the display screen
  commit        Commit all changes made in this session
  do            Run commands from Exec mode
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  help          Description of the interactive help system
  revert        Revert changes
  service       Service Commands
  show          Show running system information
  write         Write running configuration to memory or terminal

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#?
```

26.3.2 meshpoint-device-commands

meshpoint-device-config-instance

The following table lists the meshpoint-device configuration mode commands:

Table 26.4 *Meshpoint-Device Config Commands*

Command	Description	Reference
acs	Enables *Automatic Channel Selection* (ACS) on this meshpoint device (access point)	*page 26-38*
exclude	Excludes neighboring mesh devices	*page 26-43*
hysteresis	Configures path selection SNR hysteresis values on this meshpoint-device (access point)	*page 26-44*
monitor	Enables monitoring of critical resource and primary port links on a meshpoint device	*page 26-46*
path-method	Configures the method used to select the path to the root node in a mesh network	*page 26-47*
preferred	Configures the preferred path parameters for a meshpoint device	*page 26-48*
root	Configures a meshpoint device as the root meshpoint	*page 26-49*
root-select	Configures this meshpoint device as the cost root	*page 26-51*
no	Negates the commands for a meshpoint device or resets values to default	*page 26-52*

26.3.2.1 acs

meshpoint-device-commands

Enables *Automatic Channel Selection* (ACS) on this meshpoint device (access point). When enabled, this feature automatically selects the best channel for a meshpoint-device radio based on the device configuration, channel conditions, and network layout.

In a wireless network deployment, it is advantageous for network devices to have the ability to operate in multiple channels and not be limited to only a single channel. Multiple channels increase the bandwidth and throughput of the wireless network. In such a scenario, each network device must have a mechanism to dynamically select a suitable channel of operation. ACS provides the required mechanism for a MCX enabled device.

Use this command to configure the ACS settings and override the default meshpoint configurations.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|ocs-
frequency|path-min|path-threshold|preferred-interface-tolerance-period|
preferred-radio-interface|priority-meshpoint|sample-count|snr-delta|signal-
threshold|tolerance-period]

acs channel-hold-time [2.4GHz|5GHz] <0-86400>

acs channel-switch-delta [2.4GHz|5GHz] <5-35>

acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|80MHz|auto]

acs ocs-duration [2.4GHz|5GHz] <20-250>

acs ocs-frequency [2.4GHz|5GHz] <1-60>

acs path-min [2.4GHz|5GHz] <100-20000>

acs path-threshold [2.4GHz|5GHz] <800-65535>

acs preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>

acs preferred-radio-interface [2.4GHz|5GHz] <0-2>

acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>

acs sample-count [2.4GHz|5GHz] <1-10>

acs snr-delta [2.4GHz|5GHz] <1-100>

acs signal-threshold [2.4GHz|5GHz] <-100-0>

acs tolerance-period [2.4GHz|5GHz] <10-600>
```

Parameters

- `acs channel-hold-time [2.4GHz|5GHz] <0-86400>`

acs	Configures ACS settings and overrides on the selected meshpoint-device

channel-hold-time [2.4GHz|5GHz] <0-86400>	Configures the minimum time, in seconds, before a periodic scan, to assess channel conditions for a meshpoint root, is triggered. • 2.4GHz – Configures the channel hold interval for the 2.4GHz radio band • 5.0GHz – Configures the channel hold interval for the 5.0GHz radio band The following keyword is common to the '2.4GHz' and '5.0GHz' bands: • <0-86400> – Specify a value from 0 - 86400 seconds. The default is 1800 seconds. A value of '0' disables periodic channel assessment.

- `acs channel-switch-delta [2.4GHz|5GHz] <5-35>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
channel-switch-delta [2.4GHz|5GHz] <5-35>	Configures the difference in interference between the current and best channel needed to trigger a channel change. Once the difference in the current channel and the best channel interference equals the configured value, a channel change is triggered. • 2.4GHz – Configures the channel switch delta for the 2.4GHz radio band • 5.0GHz – Configures the channel switch delta for the 5.0GHz radio band The following keyword is common to the '2.4GHz' and '5.0GHz' bands: • <5-35> – Specify a value from 5 - 35 dBm. The default is 10 dBm.

- `acs channel-width [2.4GHz|5GHz] [20MHz|40MHz|80MHz|auto]`

acs	Configures ACS settings and overrides on the selected meshpoint-device
channel-width [2.4GHz|5GHz] [20MHz|40MHz|80MHz|auto]	Configures the channel width that meshpoint auto channel selection assigns to the radio • 2.4 GHz – Configures the operating channel width for the 2.4 GHz radio band • 5.0 GHz – Configures the operating channel width for the 5.0 GHz radio band The following keywords are common to the '2.4 GHz' and '5.0 GHz' bands: • 20 MHz – Assigns the 20 MHz channel width to the radio • 40 MHz – Assigns the 40 MHz channel width to the radio • 80 MHz – Assigns the 80 MHz channel width to the radio • auto – Selects and assigns the best possible channel from the 20/40/80 MHz width. This is the default setting.

- `acs ocs-duration [2.4GHz|5GHz] <20-250>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
ocs-duration [2.4GHz|5GHz] <20-250>	Configures the duration, in milliseconds, of *off -channel scans* (OCSs) • 2.4 GHz – Configures the ocs-duration for the 2.4 GHz radio band • 5.0 GHz – Configures the ocs-duration for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <20-250> – Specify a value from 20 - 250 milliseconds. The default value is 50 milliseconds.

- `acs ocs-frequency [2.4GHz|5GHz] <1-60>`

acs	Configures ACS settings and overrides on the selected meshpoint-device

ocs-frequency [2.4GHz|5GHz] <1-60>	Configures the interval, in seconds, at which off-channel scan is performed. An ocs-frequency of 10 seconds means that an off-channel scan will be performed once every 10 seconds. • 2.4 GHz – Configures the ocs-frequency for the 2.4 GHz radio band • 5.0 GHz – Configures the ocs-frequency for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-60> – Specify a value form 1 - 60 seconds. The default is 6 seconds.

- `acs path-min [2.4GHz|5GHz] <100-20000>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
path-min [2.4GHz|5GHz] <100-20000>	Configures the minimum root path metric needed for auto channel selection. This is the acceptance root path metric value to consider a root as a possible candidate mesh node. • 2.4 GHz – Configures the minimum root path metric for the 2.4 GHz radio band • 5.0 GHz – Configures the minimum root path metric for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <100-20000> – Specify a value from 100 - 20000. The default is 1000.

- `acs path-threshold [2.4GHz|5GHz] <800-65535>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
path-threshold [2.4GHz|5GHz] <800-65535>	Configures the root path metric threshold for auto channel selection. This is the acceptance root path metric threshold beyond which the root bound to is considered as bad. • 2.4 GHz – Configures the root path metric threshold for the 2.4 GHz radio band • 5.0 GHz – Configures the root path metric threshold for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <800-65535> – Specify a value from 800 - 65535. The default is 1500.

- `acs preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
preferred-interface-tolerance-period [2.4GHz|5GHz] <10-600>	Configures the maximum tolerance period, in seconds, for low root metrics on the preferred interface. This is the duration to wait before triggering an automatic channel selection for the next mesh-hop on the preferred interface. • 2.4 GHz – Configures the maximum tolerance period for the 2.4 GHz radio band • 5.0 GHz – Configures the maximum tolerance period for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <800-65535> – Specify a value from 10 - 600 seconds.

- `acs preferred-radio-interface [2.4GHz|5GHz] <0-2>`

acs	Configures ACS settings and overrides on the selected meshpoint-device

preferred-radio-interface [2.4GHz|5GHz] <0-2>	Configures the preferred radio interface on dual band APs • 2.4 GHz – Configures the preferred radio interface for the 2.4 GHz radio band • 5.0 GHz – Configures the preferred radio interface for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <0-2> – Specify a value form 0 - 2. A value of 0 (zero) indicates no preferred radio.

- `acs priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
priority-meshpoint [2.4GHz|5GHz] <MESHPOINT-NAME>	Configures the priority meshpoint. Configuring a priority meshpoint overrides automatic meshpoint configuration. • 2.4 GHz – Configures the priority meshpoint for the 2.4 GHz radio band • 5.0 GHz – Configures the priority meshpoint for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <MESHPOINT-NAME> – Specify the meshpoint name for the selected radio band.

- `acs sample-count [2.4GHz|5GHz] <1-10>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
sample-count [2.4GHz|5GHz] <1-10>	Configures the minimum number of scan cycle samples to consider for auto channel selection • 2.4 GHz – Configures the sample count for the 2.4 GHz radio band • 5.0 GHz – Configures the sample count for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-10> – Specify a value from 1 -10. The default is 5 samples.

- `acs snr-delta [2.4GHz|5GHz] <1-100>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
snr-delta [2.4GHz|5GHz] <1-100>	Configures the channel SNR delta. A meshpoint on a candidate channel must have a SNR of a greater delta than the next hop on the current channel. • 2.4 GHz – Configures the snr-delta for the 2.4 GHz radio band • 5.0 GHz – Configures the snr-delta for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <1-100> – Specify a value from 1 - 100 dB. The default is 5 dB.

- `acs signal-threshold [2.4GHz|5GHz] <-100-0>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
signal-threshold [2.4GHz|5GHz] <-100-0>	Configures the signal strength threshold. If the signal strength of the next hop drops below the configured signal-threshold, a scan is triggered. • 2.4 GHz – Configures the signal-threshold for the 2.4 GHz radio band • 5.0 GHz – Configures the signal-threshold for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <-100-0> – Specify a value from -100 - 0 dB. The default is -65 dB.

- `acs tolerance-period [2.4GHz|5GHz] <10-600>`

acs	Configures ACS settings and overrides on the selected meshpoint-device
tolerance-period [2.4GHz|5GHz] <10-600>	Configures the maximum tolerance period in seconds. This is the interval to wait for the root bound to recovery from a bad link. • 2.4 GHz – Configures the tolerance-period for the 2.4 GHz radio band • 5.0 GHz – Configures the tolerance-period for the 5.0 GHz radio band The following keyword is common to the '2.4 GHz' and '5.0 GHz' bands: • <10-600> – Specify a value from 10 - 600 seconds. the default is 60 seconds.

Example

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs channel-hold-time
2.4GHz 2500

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-duration 2.4GHz
30

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#acs ocs-frequency 2.4GHz
1

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
 meshpoint-device test
  acs ocs-frequency 2.4GHz 1
  acs osc-duration 2.4GHz 30
  acs channel-hold-time 2.4GHz 2500
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands

no	Reverts the configured ACS settings to default

26.3.2.2 exclude

meshpoint-device-commands

Enables wired-peer (that are wired MiNT level-1 neighbors) exclusion

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
exclude wired-peer mint-level-1
```

Parameters

- `exclude wired-peer mint-level-1`

exclude wired-peer	Excludes neighboring mesh devices
wired-peer mint-level-1	Excludes neighboring wired mesh devices with MiNTlevel-1 link When enabled, all neighboring wired mesh devices are excluded from mesh links.

Example

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#exclude wired-peer mint-
level-1

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
 meshpoint-device test
  exclude wired-peer mint-level-1
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands

no	Disables wired-peer exclusion on this meshpoint

26.3.2.3 hysteresis

meshpoint-device-commands

Configures path selection SNR hysteresis values on this meshpoint-device (access point). These are settings that facilitate dynamic path selection. Configuring hysteresis prevents frequent re-ranking of the shortest path cost.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]

hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-100>|
snr-delta <1-100>]
```

Parameters

```
• hysteresis [min-threshold <-100-0>|period <0-600>|root-sel-snr-delta <1-
100>|snr-delta <1-100>]
```

min-threshold <-100-0>	Configures the minimum signal strength that a device should have to be considered a likely candidate in the mesh route (to the mesh root node) selection process. • <-100-0> – Specify a value from -100 - 0 dB. The default is 0 dB.
period <0-600>	Configures the interval, in seconds, for which a likely candidate's path method hysteresis is sustained. In other words a device capable of sustaining the signal strength for the specified period of time is a likely candidate in the mesh route (to the mesh root node) selection process. • <0-600> – Specify a value from 0 - 600 seconds. The default is 1 second.
root-sel-snr-delta <1-100>	Configures the signal strength, in dB, that a device has to sustain, within the delta range, to be considered a likely candidate in the mesh route (to the mesh root node) selection process. • <1-100> – Specify a value from 1 - 100 dB.
snr-delta <1-100>	Configures the SNR delta. The device with must have a SNR of a greater delta than its current neighbor to be considered a likely candidate in the mesh route (to the mesh root) selection process. • <1-100> – Specify a value from 1 - 100 dB. The default is 1 dB.

Example

```
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis period 15
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis root-sel-snr
-delta 12
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis snr-delta 3
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#hysteresis min-threshold
-65

rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#show context
 meshpoint-device test
  hysteresis period 15
  hysteresis snr-delta 3
  hysteresis min-threshold -65
  hysteresis root-sel-snr-delta 12
rfs4000-229D58(config-profile-testAP71XX-meshpoint-test)#
```

Related Commands

no	Removes the configured path selection SNR hysteresis values

26.3.2.4 monitor

meshpoint-device-commands

Enables monitoring of critical resource and primary port links. It also configures the action taken in case a critical resource goes down or a primary port link is lost.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
monitor [critical-resource|primary-port-link-loss] action no-root
```

Parameters

- `monitor [critical-resource|primary-port-link-loss] action no-root`

critical-resource	Enables critical resource down event monitoring
primary-port-link-loss	Enables primary port link loss event monitoring
action no-root	The following are common to all of the above: • action – Sets the action taken if a critical resource goes down or if a primary port link is lost • no-root – Changes the meshpoint to be non root (this is the action taken in case any of the above mentioned two events occur)

Example

```
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#monitor critical-
resource action no-root

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  monitor critical-resource action no-root
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Related Commands

no	Disables monitoring of critical resource and primary port links.

26.3.2.5 path-method

meshpoint-device-commands

Configures the path selection method used on a meshpoint device. This is the method used to select the route to the root node within a mesh network.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
path-method [bound-pair|mobile-snr-leaf|snr-leaf|uniform]
```

Parameters

- `path-method [bound-pair|mobile-snr-leaf|snr-leaf|uniform]`

path-method	Sets the method used to select the path to the root node in a mesh network
bound-pair	Enables a meshpoint to form an exclusive path with only one other meshpoint. Select this option to bind one mesh point connection at a time. Once established, other mesh point connenction requests are denied.
mobile-snr-leaf	Configures the path selection method as mobile-snr-leaf. When selected, the path to the root node is selected based on the *Signal-to-Noise Ratio* (SNR) to a neighboring device. This option allows meshpoint devices to select a neighbor with the strongest SNR. Meshpoint devices using the mobile-snr-leaf method are non-forwarding nodes in the meshpoint traffic. **Note:** Select this option for *Vehicular Mounted Modem* (VMM) access points or other mobile devices. **Note:** VMM is supported only on the AP7161 model access point.
snr-leaf	This option allows meshpoints to select a neighbor with the strongest SNR. It is similar to the mobile-snr-leaf option, but is not applicable to mobile devices, such as VMMs.
uniform	Indicates the path selection method is uniform. When selected, two paths will be considered equivalent if the average goodput is the same for both paths. This is the default setting. **Note:** Select this option for infrastructure devices.

Example

```
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#path-method
mobile-snr-leaf

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device TEST
  name TEST
  path-method mobile-snr-leaf
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Related Commands

no	Resets the path selection method on a meshpoint device

26.3.2.6 preferred

meshpoint-device-commands

Configures the preferred path parameters for this meshpoint device

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]
```

Parameters

- `preferred [neighbor <MAC>|root <MAC>|interface [2.4GHz|4.9GHz|5GHz]]`

preferred	Configures the preferred path parameters
neighbor <MAC>	Adds the MAC address of a neighbor meshpoint as a preferred neighbor
root <MAC>	Adds the MAC address of a root meshpoint as a preferred root
interface [2.4GHz|4.9GHz|5GHz]	Sets the preferred interface

Example

```
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred
neighbor 11-22-33-44-55-66

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred root
22-33-44-55-66-77

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#preferred
interface 5GHz

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

Related Commands

no	Removes the configuration of preferred paths for this meshpoint device

26.3.2.7 root

meshpoint-device-commands

Configures this meshpoint device as the root meshpoint

You can optionally use the select-method option to enable dynamic mesh selection. When enabled, this option overrides root or no-root configuration and uses the selection method.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
root {select-method [auto-mint|auto-proximity]}
```

Parameters

- `root {select-method [auto-mint|auto-proximity]}`

root	Configures this meshpoint device as the root meshpoint
select-method auto-mint	Optional. Enables dynamic mesh selection. When enabled, this option overrides root or no-root configuration and chooses the selection method. • auto-mint – Enables dynamic root selection using Auto-MiNT (based on path cost) The Auto-Mint or Cost Method dynamically determines the root/non-root configuration of a meshpoint by: • Monitoring and ranking the signal strength and path cost of neighboring mesh points. • Setting the configuration to: • non-root: If the link with the shortest path to the cost-root mesh device is a MCX meshpoint link • root: If the link with the shortest path to the cost-root mesh device is a non MCX meshpoint link (wired link). • This requires that the meshpoint device, in the brain car, be configured as the 'cost root' and the 'cost root' meshpoint-device be the l2 gateway to the controller. Use the *root-select > cost-root* command to configure a meshpoint-device as 'cost-root'. • Using signal strength of neighboring meshpoint as the sole metric to determine the next mesh hop to the root. • Loop detection with both meshpoints in a car select non-root and form a mesh link with the same root • auto-proximity – Enables dynamic root selection using meshpoint proximity. When auto-proximity is selected, root selection is based on signal strength of candidate roots.

Example

```
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#root

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  root
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root select-method
 auto-mint

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context
 meshpoint-device test
  root select-method auto-mint
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#
```

Related Commands

no	Removes the configuration of this meshpoint device as a root meshpoint. Also allows you to disable dynamic mesh selection (if enabled).

26.3.2.8 root-select

meshpoint-device-commands

Configures this meshpoint device as the cost root

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
root-select cost-root
```

Parameters

- `root-select cost-root`

root-select cost-root	Configures this meshpoint device as the cost root. This is necessary for dynamic root selection process. Select this option to set the meshpoint as the cost root for meshpoint root selection. This setting is disabled by default.

Example

```
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#root-select cost-
root

ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#show context
 meshpoint-device test
  root select-method auto-mint
  root-select cost-root
ap7131-11E6C4(config-device-00-23-68-11-E6-C4-meshpoint-test)#
```

Related Commands

no	Removes this meshpoint-device as the cost-root

26.3.2.9 no

meshpoint-device-commands

Negates the commands for a meshpoint device or resets values to default

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7522, AP7532, AP7562, AP81XX

Syntax

```
no [acs|exclude|hysteresis|monitor|path-method|preferred|root|root-select]

no acs [channel-hold-time|channel-switch-delta|channel-width|ocs-duration|
ocs-frequency|path-min|path-threshold|preferred-interface-tolerance-period|
preferred-radio-interface|priority-meshpoint|sample-count|snr-delta|signal-
threshold|tolerance-period] [2.4GHZ|5GHz]

no exclude wired-peer mint-level-1

no hysteresis [min-threshold|period|root-sel-snr-delta|snr-delta]

no monitor [critical-resource|primary-port-link-loss]

no [path-method|root {select-method}]

no root-select cost-root

no preferred [interface|root|neighbor]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes or reverts this meshpoint device settings to default based on the parameters passed

Example

```
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  root
  preferred root 22-33-44-55-66-77
  preferred neighbor 11-22-33-44-55-66
  preferred interface 5GHz
  monitor critical-resource action no-root
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no monitor
critical-resource
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no preferred
neighbor
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no root
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#no preferred
interface

rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#show context
 meshpoint-device test
  name test
  no root
  preferred root 22-33-44-55-66-77
rfs6000-37FABE(config-profile-AP71XXTestProfile-meshpoint-test)#
```

27 PASSPOINT POLICY

A passpoint policy provides an interoperable platform for streamlining Wi-Fi access to access points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

To migrate to the Passpoint policy configuration mode, use the following command:

```
<DEVICE>(config)#passpoint-policy <POLICY-NAME>

rfs4000-229D58(config)#passpoint-policy test
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#?
Passpoint Policy Mode commands:
  3gpp                    Configure a 3gpp plmn (public land mobile network) id
  access-network-type     Set the access network type for the hotspot
  connection-capability   Configure the connection capability for the hotspot
  domain-name             Add a domain-name for the hotspot
  hessid                  Set a homogeneous ESSID value for the hotspot
  internet                Advertise the hotspot having internet access
  ip-address-type         Configure the advertised ip-address-type
  nai-realm               Configure a NAI realm for the hotspot
  net-auth-type           Add a network authentication type to the hotspot
  no                      Negate a command or set its defaults
  operator                Add configuration related to the operator of the
                          hotspot
  osu                     Online signup
  roam-consortium         Add a roam consortium for the hotspot
  venue                   Set the venue parameters of the hotspot
  wan-metrics             Set the wan-metrics of the hotspot

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal

rfs4000-229D58(config-passpoint-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

27.1 passpoint-policy

PASSPOINT POLICY

The following table summarizes passpoint policy configuration mode commands:

Table 27.1 *Hotspot-Policy-Config Commands*

Command	Description	Reference
3gpp	Configures a *3rd Generation Partnership Project* (3gpp) *Public Land Mobile Network* (PLMN) ID	*page 27-3*
access-network-type	Configures the access network type element in this hotspot	*page 27-4*
connection-capability	Configures the connection capability element in this passpoint policy	*page 27-5*
domain-name	Configures the RF Domains to which this hotspot is applicable	*page 27-7*
hessid	Configures the *Homogeneous Extended Service Set Identifier* (HESSID) for a specified hotspot zone	*page 27-8*
internet	Advertises the availability of Internet access in this hotspot	*page 27-9*
ip-address-type	Advertises the IP address type used in this hotspot.	*page 27-10*
nai-realm	Configures a *Network Access Identifier* (NAI) realm name and enters its configuration mode	*page 27-12*
net-auth-type	Configures the network authentication type used in this hotspot	*page 27-18*
no	Removes or reverts passpoint policy configuration	*page 27-19*
operator	Configures the operator friendly name for this hotspot	*page 27-20*
osu	Configures an *online sign up* (OSU) SSID/provider and enters its configuration mode	*page 27-21*
roam-consortium	Configures the list of Roaming Consortium *Organization Identifiers* (OIs) supported on this hotspot	*page 27-31*
venue	Configures the venue group and type for this passpoint policy	*page 27-32*
wan-metrics	Configures the WAN performance metrics for this hotspot	*page 27-36*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

27.1.1 3gpp

passpoint-policy

Configures a *3rd Generation Partnership Project* (3GPP) *Public Land Mobile Network* (PLMN) information. The 3GPP PLMN information is a combination of the *Mobile Country Code* (MCC) and *Mobile Network Code* (MNC). This MCC and MNC combination uniquely identifies a cellular operator. For example, Telstar Corporation Ltd. in Australia is identified by MCC 505 and MNC 001.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}
```

Parameters

- `3gpp mcc <MOBILE-COUNTRY-CODE> mnc <MOBILE-NETWORK-CODE> {description <LINE>}`

3gpp	Configures the 3GPP PLMN information that is returned in response to an ANQP query
mcc <MOBILE-COUNTRY-CODE>	Specifies the MCC. The MCC is a two or three digit decimal value. For example, the MCC for Australia is 505.
mnc <MOBILE-NETWORK-CODE>	Specifies the MNC. The MNC is a two or three decimal value used in combination with the MCC to uniquely identify a mobile network operator. The MNC and MCC combination (also known as the MCC/MNC tuple) forms the first five or six digits of the *International Mobile Subscriber's Identity* (IMSI). If the MCC and MNC values are not configured, the hotspot will not return the element in an ANQP capability request and ignores any ANQP query for the element.
description <LINE>	Optional. Configures a description that uniquely identifies this PLMN. Provide a description not exceeding 64 characters in length.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 505 mnc 14

rfs4000-229D58(config-passpoint-policy-test)#3gpp mcc 310 mnc 970

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the specified 3gpp PLMN information and its corresponding MCC/MNC settings

27.1.2 access-network-type

passpoint-policy

Configures the access network type for this hotspot. The beacons and probe responses communicate the type of hotspot (public, private, guest-use, emergency, etc.) to clients seeking access.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
access-network-type [chargeable-public|emergency-services|experimental|free-public|personal-device|private|private-guest|wildcard]
```

Parameters

```
• access-network-type [chargeable-public|emergency-services|experimental|free-public|personal-device|private|private-guest|wildcard]
```

access-network-type	Select the access network type for this hotspot. The options are: • chargeable-public – The network type is a chargeable public network • emergency-services – The network is used to provide emergency services only • experimental – The network is used for test or experimental purposes only • free-public – The network type is a free public • personal-device – The network is used for personal devices only • private – The network is a private network • private-guest – The network is a private network with guest access (default setting) • wildcard – Includes all access network types If the network type is set to chargeable-public, probe responses advertise this hotspot as a chargeable-public hotspot.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#access-network-type chargeable-public

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Reverts to the default access network type setting (private)

27.1.3 connection-capability

passpoint-policy

Configures the connection capability element in this passpoint policy. When configured, it communicates which ports are open or closed on the Hotspot, in response to an ANQP query.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
connection-capability [ftp|http|icmp|ip-protocol|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn]

connection-capability [ftp|http|icmp|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn] [closed|open|unknown]

connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]
```

Parameters

- `connection-capability [ftp|http|icmp|ipsec-vpn|pptp-vpn|sip|ssh|tls-vpn] [closed|open|unknown]`

connection-capability	Configures the connection capability element in this passpoint policy
ftp	Specifies the protocol type as FTP. Configures TCP port 20.
http	Specifies the protocol type as HTTP. Configures TCP port 80.
icmp	Specifies the protocol type as ICMP
ipsec-vpn	Specifies the protocol type as IPSEC VPN. Configures ESP and UDP ports 500 and 4500.
pptp-vpn	Specifies the protocol type as PPTP VPN. Configures TCP port 1723.
sip	Specifies the protocol type as SIP. Configures TCP port 5060 and UDP port 5060.
ssh	Specifies the protocol type as SSH. Configures TCP port 20
tls-vpn	Specifies the protocol type as TLS VPN. Configures TCP port 443.
port <0-65535> [closed|open|unknown	After specifying the protocol type, specify the port (associated with the selected protocol) and its status. • closed – Specifies that the port(s) is/are closed • open – Specifies that the port(s) is/are open • unknown – Specifies that the port(s) status is not known When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.

- `connection-capability ip-protocol <0-255> port <0-65535> [closed|open|unknown]`

connection-capability	Configures the connection capability element in this passpoint policy
ip-protocol <0-255>	Identifies the IP protocol by the protocol's number. For example, for *simple message protocol* (SMP) specify 121.

port <0-65535> [closed|open|unknown	After specifying the IP protocol type, specify the port number. • port <0-65535> – Select a port for the IP protocol identified. After specifying the port number, specify the port status. • closed – Specifies that the port(s) is/are closed • open – Specifies that the port(s) is/are open • unknown – Specifies that the port(s) status is not known When the connection capability element is not configured, the hotspot does not return the element in an ANQP capability request and ignores any ANQP query for the element.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#connection-capability 1 ip-protocol
2 port 10 closed

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the configured connection capability element on the passpoint policy

27.1.4 domain-name

passpoint-policy

Configures the RF Domain(s) that are returned in response to an ANQP query

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
domain-name <DOMAIN-NAME>
```

Parameters

- `domain-name <DOMAIN-NAME>`

domain-name <DOMAIN-NAME>	Specify the RF Domain name An hotspot can be applied across multiple RF Domains.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#domain-name TechPubs

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the RF Domain mapped to this passpoint policy

27.1.5 hessid

passpoint-policy

Configures the *Homogeneous Extended Service Set Identifier* (HESSID) for the hotspot. The HESSID uniquely identifies a hotspot provider within a zone. This is essential in zones (such as an airport or shopping mall) having multiple hotspot service providers with overlapping coverage.

An HESSID is a 6 (six) byte identifier that uniquely identifies a set of APs belonging to the same network and exhibiting same network behavior. It is the BSSID (MAC address) of one of the devices (AP) in the zone. When not configured, the radio's BSSID is used as the HESSID.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
hessid <MAC>
```

Parameters

- `hessid <MAC>`

hessid <MAC>	Specify a unique 6 (six) byte identifier for this passpoint policy.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#hessid 00-23-68-88-0D-A7

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the HESSID configured with this passpoint policy and reverts back to using the radio's BSSID

27.1.6 internet

passpoint-policy

Advertises the availability of Internet access on this hotspot. The Internet bit in the hotspot's beacon and probe responses indicates if Internet access is available or not. By default this feature is enabled.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
internet
```

Parameters

None

Example

```
rfs4000-229D58(config-passpoint-policy-test)#internet
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes Internet access on this passpoint policy

27.1.7 ip-address-type

passpoint-policy

Advertises the IP address type used in this hotspot. This information is returned in response to ANQP queries.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
ip-address-type [ipv4|ipv6]

ip-address-type ipv4 [double-nat|not-available|port-restricted|port-restricted-double-nat|port-restricted-single-nat|public|single-nat|unknown]

ip-address-type ipv6 [available|not-available|unknown]
```

Parameters

- `ip-address-type ipv4 [double-nat|not-available|port-restricted|port-restricted-double-nat|port-restricted-single-nat|public|single-nat|unknown]`

ip-address-type ipv4	Configures the as IPv4 address type availability information
double-nat	Specifies double NATed private IPv4 address is available
not-available	Specifies IPv4 address is not available
port-restricted	Specifies port-restricted IPV4 address is available
port-restricted-double-nat	Specifies port-restricted IPv4 address and double NATed IPv4 address is available
port-restricted-single-nat	Specifies port-restricted IPv4 address and single NATed IPv4 address is available
public	Specifies public IPv4 address is available
single-nat	Specifies single NATed IPv4 address is available
unknown	Specifies no information configured regarding the IPv4 address availability

- `ip-address-type ipv6 [available|not-available|unknown]`

ip-address-type ipv6	Configures the IPv6 address type availability information
available	Specifies IPv6 address is available
not-available	Specifies IPv6 address is not available
unknown	Specifies no information configured regarding the IPv6 address availability

Example

```
rfs4000-229D58(config-passpoint-policy-test)#ip-address-type ipv6 available

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the IP address type configured for this passpoint policy

27.1.8 nai-realm

passpoint-policy

A *Network Access Identifier* (NAI) realm element in the passpoint policy identifies a hotspot service provider by the unique NAI realm name.

The following table lists NAI realm configuration mode commands:

Table 27.2 *NAI-Realm-Config Commands*

Command	Description	Reference
nai-realm	Creates a NAI realm name for this hotspot and enters its configuration mode	*page 27-13*
nai-realm-config-mode commands	Invokes the NAI realm configuration mode commands	*page 27-15*

27.1.8.1 nai-realm

nai-realm

Configures a NAI realm name and enters its configuration mode. The NAI realm name identifies the accessible hotspot service providers. You can configure a list of NAI realm names of service providers operating within a specific hotpsot zone.This NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query.

The configured NAI realm name list is presented in ANQP response to a NAI realm and NAI home realm query.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
nai-realm <HOTSPOT2-NAI-REALM-NAME>
```

Parameters

- `nai-realm <HOTSPOT2-NAI-REALM-NAME>`

nai-realm <HOTSPOT2-NAI-REALM-NAME>	Configures the NAI realm name for this passpoint policy • <HOTSPOT2-NAI-REALM-NAME> – Specify the NAI realm name for this passpoint policy.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#nai-realm mail.example.com
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#?
Hotspot2 NAI Realm Mode commands:
  eap-method  Set an eap method
  no          Negate a command or set its defaults

  clrscr      Clears the display screen
  commit      Commit all changes made in this session
  do          Run commands from Exec mode
  end         End current mode and change to EXEC mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  revert      Revert changes
  service     Service Commands
  show        Show running system information
  write       Write running configuration to memory or terminal

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#exit
```

```
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 nai-realm mail.example.com
 nai-realm mail.testrealm.com
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the NAI realm name configured for this passpoint policy

27.1.8.2 nai-realm-config-mode commands

nai-realm

The following table summarizes NAI realm configuration mode commands:

Table 27.3 *NAI-Realm-Config-Mode Commands*

Command	Description	Reference
eap-method	Specifies the *Extensible Authentication Protocol* (EAP) authentication mechanisms supported by each of the service providers associated with this passpoint policy	*page 27-16*

27.1.8.2.1 eap-method

nai-realm-config-mode commands

Specifies the EAP authentication mechanisms supported by each of the service providers associated with this passpoint policy

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
eap-method <1-10> [<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|peap|
psk|rsa-public-key|sim|tls|ttls] auth-param [credential|expanded-eap|
expanded-inner-eap|inner-eap|non-eap-inner|tunn-eap-credential|vendor] [cert|hw-
token|nfc-secure-elem|none|sim|soft-token|username-password|usim|vendor]
```

Parameters

```
• eap-method <1-10> [<1-255>|fast|gtc|identity|ikev2|ms-auth|mschapv2|otp|peap|
psk|rsa-public-key|sim|tls|ttls] auth-param [credential|expanded-eap|expanded-
inner-eap|inner-eap|non-eap-inner|tunn-eap-credential|vendor][cert|hw-token|nfc-
secure-elem|none|sim|soft-token|username-password|usim|vendor]
```

eap-method <1-10>	Creates an EAP authentication method and assigns it an index number • <1-10> – Specify a identifier for this EAP method from 1 - 10. A maximum of 10 (ten) authentication methods can be specified for every NAI realm. After creating the EAP authentication method, specify the associated authentication mechanisms (method types).
<1-255>	Identifies the EAP authentication method type from the corresponding *Internet Assigned Numbers Authority* (IANA) number <1-255> – Specify the IANA identity number for the authentication protocol from 1 - 255.
fast	Specifies the EAP authentication method type as *Flexible Authentication via Secure Tunneling* (FAST)
gtc	Specifies the EAP authentication method type as *Generic Token Card* (GTC)
identity	Specifies the EAP authentication method type as Identification
ikev2	Specifies the EAP authentication method type as *Internet Key Exchange Protocol version 2* (IKEv2)
ms-auth	Specifies the EAP authentication method type as *Microsoft Authentication* (MS-Auth)
mschapv2	Specifies the EAP authentication method type as *Microsoft Challenge Handshake Authentication Protocol* version 2(MSCHAPv2)
opt	Specifies the EAP authentication method type as *One Time Password* (OTP)
peap	Specifies the EAP authentication method type as *Protected Extensible Authentication Protocol* (PEAP)
psk	Specifies the EAP authentication method type as *Pre-shared Key* (PSK)
rsa-public-key	Specifies the EAP authentication method type as RSA public key protocol
sim	Specifies the EAP authentication method type as GSM *Subscriber Identity Module* (SIM)

tls	Specifies the EAP authentication method type as *Transport Layer Security* (TLS)
ttls	Specifies the EAP authentication method type as *Tunneled Transport Layer Security* (TTLS)
auth-param	After specifying the EAP authentication method type, specify the authentication parameters. These parameters depend on the EAP authentication mechanism selected.
[cert|hw-token| nfc-secure-elem| none|sim|soft-token| username-password| usim|vendor]	The following parameters are common to all the above authentication parameters: • cert – Certificate • hw-token – Hardware token • nfc-secure-elem – NFC secure element • none – No credential • sim – Subscriber identity module • soft-token – Soft token • username-password – Username and password • usim – Universal subscriber identity module • vendor – Vendor specific credential

Example

The following examples show four EAP authentication methods associated with the NAI realm 'mail.example.com'. Each method supports a different EAP authentication mechanism:

```
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-
method 1 ttls auth-param vendor hex 00001E

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-
method 2 rsa-public-key auth-param credential cert


rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#eap-
method 4 peap auth-param credential cert

rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#show
context
 nai-realm mail.example.com
  eap-method 1 ttls auth-param vendor hex 00121F
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
rfs4000-229D58(config-passpoint-policy-test-nai-realm-mail.example.com)#
```

27.1.9 net-auth-type

passpoint-policy

Configures the network authentication type used in this hotspot. The details configured are returned in response to an ANQP query.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
net-auth-type [accept-terms|dns-redirect|http-redirect|online-enroll] {url <URL>}
```

Parameters

```
• net-authtype [accept-terms|dns-redirect|http-redirect|online-enroll] {url
<URL>}
```

net-auth-type	Specifies the network authentication type used with this passpoint policy. The options are: accept-terms, dns-redirect, http-redirect, and online-enroll
accept-terms	Enables user acceptance of terms and conditions
dns-redirect	Enables DNS redirection of user
http-redirect	Enables HTTP redirection of user
online-enroll	Enables online user enrolment
url <URL>	Optional. Specify the location for each of above network authentication types.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#net-auth-type accept-terms url
"www.test.com"
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 nai-realm mail.example.com
  eap-method 1 ttls auth-param vendor hex 00001E
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
 nai-realm mail.testrealm.com
 net-auth-type accept-terms url www.test.com
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the network authentication type configured with this passpoint policy

27.1.10 no

passpoint-policy

Removes or reverts the passpoint policy settings

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
no [3gpp|access-network-type|connection-capability|domain-name|hessid|internet|
ip-address-type|nai-realm|net-auth-type|operator|osu|roam-consortium|venue|wan-
metrics]
```

Parameters

- `no` <PARAMETERS>

no <PARAMETERS>	Removes or reverts the passpoint policy settings

Example

The following example shows the passpoint policy 'test' settings before the 'no' commands are executed:

```
rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 access-network-type chargeable-public
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 hessid 00-23-68-88-0D-A7
 ip-address-type ipv6 available
 nai-realm mail.example.com
  eap-method 1 ttls auth-param vendor hex 00001E
  eap-method 2 rsa-public-key auth-param credential cert
  eap-method 3 otp auth-param credential username-password
  eap-method 4 peap auth-param credential cert
 nai-realm mail.testrealm.com
 net-auth-type accept-terms url www.test.com
 3gpp mcc 310 mnc 970
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#

rfs4000-229D58(config-passpoint-policy-test)#no access-network-type
rfs4000-229D58(config-passpoint-policy-test)#no hessid
rfs4000-229D58(config-passpoint-policy-test)#no nai-realm mail.example.com
rfs4000-229D58(config-passpoint-policy-test)#no 3gpp mcc 310 mnc 970
rfs4000-229D58(config-passpoint-policy-test)#no internet

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.test.com
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

27.1.11 operator

passpoint-policy

Configures the operator friendly name for this hotspot. The name can be configured in English or in any language other than English. When the name is specified in English, the system allows an ASCII input. If you are using a language other than English, first specify the ISO-639 language code, and then specify the name as an hexadecimal code.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
operator name <OPERATOR-NAME>
```

Parameters

- `operator name <OPERATOR-NAME>`

name <OPERATOR-NAME>	Configures the operator's name in English • <OPERATOR-NAME> – Specify the operator friendly name in ASCII format.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#operator name emergencyservices

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.test.com
 operator name emergencyservices
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the operator friendly name configured for this passpoint policy

27.1.12 osu

passpoint-policy

The following table lists the OSU SSID/provider configuration commands:

Table 27.4 *OSU-SSID/Provider Config Commands*

Command	Description	Reference
osu	Configures an *online sign up* (OSU) SSID/provider and enters its configuration mode	*page 27-22*
osu-config-mode commands	Summarizes the OSU SSID/provider configuration mode commands	*page 27-23*

27.1.12.1 osu

osu

Adds an *online sign up* (OSU) SSID (WLAN)/OSU provider and enters its configuration mode

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
osu [provider <PASSPOINT-OSU-PROVIDER>|ssid <SSID>]
```

Parameters

- `osu [provider <PASSPOINT-OSU-PROVIDER>|ssid <SSID>]`

osu	Use this command to configure an *online sign up* (OSU) SSID/OSU provider. In the OSU SSID/provider configuration mode, specify OSU details, such as names, descriptions, servers, methods, and icons available. This information is returned in response to a station's Hotspot 2.0 query. When configured, this option enables a station to obtain credentials for an Hotspot 2.0 enabled SSID.
provider <PASSPOINT-OSU-PROVIDER>	Creates an OSU provider for this passpoint and enters its configuration mode • <PASSPOINT-OSU-PROVIDER> – Specify an identification for this OSU passpoint provider.
ssid <SSID>	Configures an OSU WLAN's SSID. This is the open authentication SSID that a user can use to obtain credentials for the passpoint SSID. • <SSID> – Specify the SSID.

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#?
Passpoint OSU Provider Mode commands:
  description  Configure the english description of the online signup provider
  icon         Add an icon for the online signup provider
  method       Specify the online signup method supported by provider
  nai          Configure the NAI for the online signup provider
  name         Configure the english name of the online signup provider
  no           Negate a command or set its defaults
  server-url   Configure the signup url for the online signup provider

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes the OSU WLAN/provider configured with this passpoint policy

27.1.12.2 osu-config-mode commands

osu

The following table summarizes OSU SSID/provider configuration mode commands:

Table 27.5 *OSU-SSID/Provider-Config-Mode Commands*

Command	Description	Reference
description	Configures the OSU provider's description	*page 27-24*
icon	Adds the OSU provider's icon	*page 27-25*
method	Configures the open sign up methods available on this OSU provider	*page 27-26*
nai	Configures the OSU provider's NAI	*page 27-27*
name	Configures the OSU provider's name	*page 27-28*
no	Removes the settings configured for this OSU provider	*page 27-29*
server-url	Configures the OSU provider server's URL	*page 27-30*

27.1.12.2.2 description

osu-config-mode commands

Configures the OSU SSID/provider's description. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
description [<DESCRIPTION>|iso-lang <ISO-LANG-CODE>]
```

Parameters

- `description [<DESCRIPTION>|iso-lang <ISO-LANG-CODE>]`

<DESCRIPTION>	Provides a description for the OSU provider. It should not exceed 253 characters in length. • <DESCRIPTION> – Specify the description in one or more languages. By default the system configures the name in English.
iso-lang <ISO-LANG-CODE>	Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). By default the language is set to English. If specifying the description in any language other than English, specify the ISO language code.

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#description
"Provides free service for testing purposes"

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  description "Provides free service for testing purposes"
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes this OSU provider's description

27.1.12.2.3 icon

osu-config-mode commands

Adds the OSU provider's icon. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
icon iso-lang <ISO-LANG-CODE> width <0-65535> height <0-65535> mime-type <FILE-MIME-TYPE> file [<IMAGE-FILE-NAME/PATH>|<FILE-NAME>]
```

Parameters

```
• icon iso-lang <ISO-LANG-CODE> width <0-65535> height <0-65535> mime-type <FILE-MIME-TYPE> file [<IMAGE-FILE-NAME/PATH>|<FILE-NAME>]
```

icon iso-lang <ISO-LANG-CODE>	Configures an icon representing the OSU provider • iso-lang <ISO-LANG-CODE> – Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). By default the language is set to English. If specifying the image file name and path in any language other than English, specify the ISO language code.
width <0-65535>	Configures the icon's width in pixels • <0-65535> – Specify a value from 0 - 65535 pixels.
height <0-65535>	Configures the icon's height in pixels • <0-65535> – Specify a value from 0 - 65535 pixels.
mime-type <FILE-MIME-TYPE>	Configures a string describing the icon's standard mime type. For example, image/png • <FILE-MIME-TYPE> – Specify the icon's mime type.
file [<IMAGE-FILE-NAME/ PATH>|<FILE-NAME>]	Configures the location and name of the image file • <IMAGE-FILE-NAME/PATH> – Specify the path and filename. For example, flash:/ icon.png • <FILE-NAME> – Use this option to specify the filename in the flash:/ directory

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#icon iso-lang eng
width 128 height 128 mime-type image/png file flash:/wifi_icon

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes this OSU provider's icon

27.1.12.2.4 method

osu-config-mode commands

Configures the open sign up methods available on this OSU provider. This value is returned, in the specified order of precedence, in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
method [oma-dm|soap-xml-spp] priority <1-2>
```

Parameters

- `method [oma-dm|soap-xml-spp] priority <1-2>`

method [oma-dm|soap-xml-spp] priority <1-2>	Configures the online sign up methods supported by this OSU provider • oma-dm – Configures the OSU method used as *Open Mobile Alliance* (OMA) device management • soap-xml-spp – Configures the OSU method used as Soap-xml subscription provisioning protocol • priority <1-2> – Sets the priority of the specified method. Select a value from 1 - 2. The default is one (1).

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#method soap-xml-spp
priority 1

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
  method soap-xml-spp priority 1
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes the online sign up methods configured on this OSU provider

27.1.12.2.5 nai

osu-config-mode commands

Configures the OSU provider's NAI. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
nai <WORD>
```

Parameters

- `nai <WORD>`

nai <WORD>	Configures the OSU provider's NAI • <WORD> – Specify the NAI.

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#nai wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
  method soap-xml-spp priority 1
  nai wifi.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes this OSU provider's NAI

27.1.12.2.6 name

osu-config-mode commands

Configures the OSU provider's name. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
name [<NAME>|iso-lang <ISO-LANG-CODE>]
```

Parameters

- `name [<NAME>|iso-lang <ISO-LANG-CODE>]`

<NAME>	Configures the OSU provider's name. It should not exceed 253 characters in length. • <NAME> – Specify the name in one or more languages. By default the system configures the name in English.
iso-lang <ISO-LANG-CODE>	Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). By default the language is set to English. If specifying the name in any language other than English, specify the ISO language code.

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#name "WIFI Alliance
OSU"

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFI
  name "WIFI Alliance OSU"
  description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
  method soap-xml-spp priority 1
  nai wifi.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes this OSU provider's name

27.1.12.2.7 no

osu-config-mode commands

Removes the settings configured for this OSU provider. Once removed the information is not included in the ANQP providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
no [description|icon|method|nai|name|server-url]

no [description|icon|name] {iso-lang <ISO-LANG-CODE>}

no [nai|server-url]

no method [oma-dm|soap-xml-spp]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes the settings configured for this OSU provider

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  name "WIFI Alliance OSU"
  description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
  method soap-xml-spp priority 1
  nai wifi.org
  server-url osu-server.wifi.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#no description
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#no icon iso-lang
eng
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#no name
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  method soap-xml-spp priority 1
  nai wifi.org
  server-url osu-server.wifi.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

27.1.12.2.8 server-url

osu-config-mode commands

Configures the OSU provider server's URL. This value is returned in the ANQP OSU providers list.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
server-url <URL>
```

Parameters

- `server-url <URL>`

server-url <URL>	Configures the OSU provider server's URL • <URL> – Specify the server's url.

Example

```
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#server-url
osu-server.wifi.org

nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#show context
 osu provider WiFi
  name "WIFI Alliance OSU"
  description "Provides free service for testing purposes"
  icon iso-lang eng width 128 height 128 mime-type image/png file flash:/wifi_icon
  method soap-xml-spp priority 1
  nai wifi.org
  server-url osu-server.wifi.org
nx9500-6C8809(config-passpoint-policy-test-osu-provider-WiFi)#
```

Related Commands

no	Removes this OSU provider's server's URL

27.1.13 roam-consortium

passpoint-policy

Configures a list of *Roaming Consortium* (RC) *Organization Identifiers* (OIs) supported on this hotspot. The beacons and probe responses communicate this Roaming Consortium list to devices. This information enables a device to identify the networks available through this AP.

Each OI identifies a either a group of *Subscription Service Providers* (SSPs) or a single SSP.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
roam-consortium hex <WORD>
```

Parameters

- `roam-consortium hex <WORD>`

roam-consortium hex <WORD>	Adds a Roaming Consortium OI to this hotspot in hexadecimal format • <WORD> – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)
hex <WORD>	Configures a hexadecimal input • <WORD> – Specify the Roaming Consortium OI in hexadecimal format (should not exceed 128 characters)

Example

```
rfs4000-229D58(config-passpoint-policy-test)#roam-consortium hex 223344

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.test.com
 operator name emergencyservices
 roam-consortium hex 223344
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the Roaming Consortium OIs supported on this passpoint policy

27.1.14 venue

passpoint-policy

Configures the venue where this hotspot is located. The hotspot venue configuration informs prospective clients about the hotspot's nature of activity, such as educational, institutional, residential, etc.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
venue [group|name]

venue group [assembly|business|educational|industrial|institutional|mercantile|
outdoor|residential|storage|unspecified|utility-and-misc|vehicular] type

venue name [<VENUE-NAME>|iso-lang]
venue name <VENUE-NAME>
venue name iso-lang <ISO-LANG-CODE> <VENUE-NAME>
```

Parameters

```
• venue group
[assembly|business|educational|industrial|institutional|mercantile|outdoor|resid
ential|storageunspecified|utility-and-misc|vehicular] type
```

venue group	Configures the venue group associated with this hotspot
assembly type	Configures the venue group as assembly (1). This hotspot type is applicable to public assembly venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • amphitheater – Specifies the venue type as amphitheater (4) • amusement-park – Specifies the venue type as amusement park (5) • arena – Specifies the venue type as arena (1) • bar – Specifies the venue type as bar (12) • coffee-shop – Specifies the venue type as a coffee shop (13) • convention-centre – Specifies the venue type as a convention center (7) • emergency-coordination-center – Specifies the venue type as a emergency coordination center (15) • library – Specifies the venue type as a library (8) • museum – Specifies the venue type as a museum (9) • passenger-terminal – Specifies the venue type as a passenger terminal (3) • place-of-worship – Specifies the venue type as a place of worship (6) • restaurant – Specifies the venue type as a restaurant (10) • stadium – Specifies the venue type as a stadium (2) • theater – Specifies the venue type as a theater (11) • unspecified – Specifies the venue type as not specified (0) • zoo – Specifies the venue type as a zoo (14)

business type	Configures the venue group as business (2). This hotspot type is applicable to business venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • attorney – Specifies the venue type as the attorney's office (9) • bank – Specifies the venue type as a bank (2) • doctor – Specifies the venue type as a doctor or dentist's office (1) • fire-station – Specifies the venue type as a fire station (3) • police-station – Specifies the venue type as a police station (4) • post-office – Specifies the venue type as a post office (5) • professional-office – Specifies the venue type as a professional office (7) • research-and-development-facility – Specifies the venue type as a research facility (8) • unspecified – Specifies the venue type as not specified (0)
educational	Configures the venue group as educational (3). This hotspot type is applicable to educational institutions. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • school-primary – Specifies the venue type as a primary school (1) • school-secondary – Specifies the venue type as a secondary school (2) • university – Specifies the venue type as a university or college (3) • unspecified – Specifies the venue type as not specified (0)
industrial	Configures the venue group as industrial (4). This hotspot type is applicable to industrial venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • factory – Specifies the venue type as a factory (1) • unspecified – Specifies the venue type as not specified (0)
institutional	Configures the venue group as institutional (4). This hotspot type is applicable to public health and other institutions. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • group-home – Specifies the venue type as a group-home (4) • hospital – Specifies the venue type as a hospital (1) • long-term-care – Specifies the venue type as a long term care facility (2) • prison – Specifies the venue type as a prison or jail (5) • rehab – Specifies the venue type as a rehabilitation facility (3) • unspecified – Specifies the venue type as not specified (0)
mercantile	Configures the venue group as mercantile (6). This hotspot type is applicable to public mercantile venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • automotive – Specifies the venue type as a automotive service center (3) • gas-station – Specifies the venue type as a gas station (5) • grocery – Specifies the venue type as a grocery store (2) • mall – Specifies the venue type as a shopping mall (4) • retail – Specifies the venue type as a retail store (1) • unspecified – Specifies the venue type as not specified (0)

outdoor	Configures the venue group as outdoor (11). This hotspot type is applicable to public outdoor venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • bus-stop – Specifies the venue type as a bus stop (5) • city-park – Specifies the venue type as a city park (2) • kiosk – Specifies the venue type as a kiosk (6) • muni-mesh – Specifies the venue type as a muni-mesh (municipal wireless Wi-Fi) (1) • rest-area – Specifies the venue type as a rest area (3) • traffic-control – Specifies the venue type as a traffic control area (4) • unspecified – Specifies the venue type as not specified (0)
residential	Configures the venue group as residential (7). This hotspot type is applicable to residential complexes. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • boarding-house – Specifies the venue type as a boarding-house (4) • dorm – Specifies the venue type as a dormitory (3) • hotel – Specifies the venue type as a hotel or motel (2) • private – Specifies the venue type as a private residence (1) • unspecified – Specifies the venue type as not specified (0)
storage	Configures the venue group as storage (8). This hotspot type is applicable to storage groups. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
unspecified	Configures the venue group as unspecified (0) • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
utility-and-misc	Configures the venue group as utility and miscellaneous (8) • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • unspecified – Specifies the venue type as not specified (0)
vehicular	Configures the venue group as vehicular (7). This hotspot type is applicable to mobile venues. • type – Specifies the venue type for this group. The options are: • <0-255> – Specifies an unlisted venue type number from 0 -255 • airplane – Specifies the venue type as an airplane (2) • auto – Specifies the venue type as an automobile or truck (1) • bus – Specifies the venue type as a bus (3) • ferry – Specifies the venue type as a ferry (5) • motor-bike – Specifies the venue type as a motor bike (7) • ship – Specifies the venue type as a ship or boat (5) • train – Specifies the venue type as a train (6) • unspecified – Specifies the venue type as not specified (0)

- `operator name <VENUE-NAME>`

name <WORD>	Configures the venue name in English • <WORD> – Specify the venue name in ASCII format.

- `operator name iso-lang <ISO-LANG-CODE> <VENUE-NAME>`

name iso-lang <ISO-LANG-CODE> <VENUE-NAME>	Configures a non-English venue name • iso-lang <ISO-LANG-CODE> – Identifies the language by its ISO 639 language code (for example, 'chi-chinese' or 'spa-spanish'). • <ISO-LANG-CODE> – Specify the 3 character iso-639 language code (for example, 'chi-chinese' or 'spa-spanish'). • <VENUE-NAME> – Specifies the venue name as a hexadecimal code

Example

```
rfs4000-229D58(config-passpoint-policy-test)#venue name PublicSchool

rfs4000-229D58(config-passpoint-policy-test)#venue group assembly type coffee-
shop

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.test.com
 operator name emergencyservices
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name PublicSchool
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the venue group and type configured with this passpoint policy

27.1.15 wan-metrics

passpoint-policy

Configures the WAN performance metrics for this hotspot. This command configures the upstream and downstream speeds associated with this hotspot. The upstream and downstream speed values (in Kbps) are estimates of the bandwidth available on the WAN. This information is returned in response to client ANQP query, and is useful for clients having a minimum and/or large bandwidth requirement.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms —NX7500, NX7510, NX7520, NX7530, NX95XX, NX9600, VX9000

Syntax

```
wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>
```

Parameters

- `wan-metrics down-speed <0-4294967295> up-speed <0-4294967295>`

wan-metrics	Specifies the WAN metrics for the up and down traffic
down-speed <0-4294967295>	Configures the down stream traffic speed • <0-4294967295> – Specify a value from 0 - 4294967295 Kbps.
up-speed <0-4294967295>	Configures the up stream traffic speed • <0-4294967295> – Specify a value from 0 - 4294967295 Kbps.

Example

```
rfs4000-229D58(config-passpoint-policy-test)#wan-metrics down-speed 2000 up-speed
2000

rfs4000-229D58(config-passpoint-policy-test)#show context
hotspot2-policy test
 connection-capability ip-protocol 2 port 10 closed
 domain-name TechPubs
 no internet
 ip-address-type ipv6 available
 nai-realm mai.testrealm.com
 net-auth-type accept-terms url www.test.com
 operator name emergencyservices
 roam-consortium hex 223344
 venue group assembly type coffee-shop
 venue name PublicSchool
 wan-metrics down-speed 2000 up-speed 2000
 3gpp mcc 505 mnc 14
rfs4000-229D58(config-passpoint-policy-test)#
```

Related Commands

no	Removes the WAN metrics configuration on this passpoint policy

28 BORDER GATEWAY PROTOCOL

This chapter summarizes the *Border Gateway Protocol* (BGP) related configuration commands in the CLI command structure.

BGP is a routing protocol, which establishes routing between ISPs. ISPs use BGP to exchange routing information between *Autonomous Systems* (ASs) on the Internet. The routing information shared includes details, such as ASs traversed to a particular destination, reachable ASs, best paths available, network policies and rules applied on a route, etc. These details appear as BGP attributes carried in routing update packets. BGP uses this information to make routing decisions. Therefore, the primary role of a BGP system is to exchange routing information with other BGP peers.

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a *graceful* close (all outstanding data is delivered before the connection is closed). Routing information exchanged through BGP supports only destination-based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

An AS is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. There are two types of BGP systems: *external BGP* (eBGP) and *internal BGP* (iBGP). iBGP represents the exchange of routing information between BGP peers within an AS. Whereas, when two BGP peers, belonging to different ASs, are connected you have an eBGP setup.

BGP peers (also referred to as neighbors) are BGP enabled devices that are directly connected through an established TCP connection. When two BGP enabled peers establish a TCP connection the first time, they exchange their BGP routing tables. All subsequent route table modifications are exchanged as route updates. BGP tracks these route updates by maintaining route table version numbers. With every update the version number changes. At any given point in time, all BGP peers should have the same route table version. The peer-to-peer TCP connections are kept alive through keepalive packets exchanged at specified intervals. Errors and special events are communicated between peers as notification packets.

This chapter is organized as follows:

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

28.1 bgp-ip-prefix-list-config commands

BORDER GATEWAY PROTOCOL

IP prefix lists are a convenient way to filter prefixes (contained in route update packets) transmitted to (or received from) other BGP supported routers. IP prefix lists are similar to access lists. They contain ordered entries (deny or permit prefix rules), identified by their sequence numbers. Each rule specifies match criteria (network and subnet prefixes and prefix masks) to match. When a prefix (received or transmitted) matches the prefix specified in one of the rules, it is filtered and an action is applied depending on where the IP prefix list is used. For example, when used in the BGP neighbor context, the prefixes received from the neighbor are filtered and the filtered prefixes are either rejected or accepted depending on the rule type (deny or permit).

IP prefix lists are also used in the BGP route map context to filter prefixes. The action applied, on filtered prefixes is set within the route map. Another use case for IP prefix lists is to filter prefixes before redistribution of local OSPF routes to eBGP enabled ASs.

Like in access lists, these deny and permit prefix rules are processed sequentially, in ascending order of their sequence number. Once a match is made, the BGP enabled router stops processing all subsequent rules in the ip-prefix-list.

IP prefix lists are used as match criteria in the following contexts:

- BGP neighbor. For more information, see *use*.
- BGP route-map context. For more information, see *match*.

To navigate to the ip-prefix-list configuration instance, use the following command:

```
<DEVICE>(config)#bgp ip-prefix-list <IP-PREFIX-LIST-NAME>

<DEVICE>(config-bgp-ip-prefix-list-test)#?
BGP IP Prefix List Mode commands:
  deny      IP Prefix deny rule to specify packets to reject
  no        Negate a command or set its defaults
  permit    IP Prefix permit rule to specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

<DEVICE>(config-bgp-ip-prefix-list-test)#
```

The following table summarizes the BGP IP prefix list configuration commands:

Table 28.1 *BGP-IP-Prefix-List-Config Commands*

Command	Description	Reference
deny	Creates and configures a deny prefix-list rule	*page 28-4*
permit	Creates and configures a permit prefix-list rule	*page 28-5*
no	Removes the specified deny or permit prefix-list rule from this IP prefix list	*page 28-6*

28.1.1 deny

bgp-ip-prefix-list-config commands

Creates and configures a deny prefix-list rule. The deny rule specifies match criteria based on which prefixes received from (or transmitted to) a BGP neighbor are filtered. A deny action is applied on these filtered prefixes. For example, in the BGP router neighbor context a filter is applied using a IP prefix list. The list contains a deny rule with a prefix to match as 192.168.13.0/24. All prefixes received from the neighbor matching this prefix are denied.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
deny prefix-list <1-4292967294> [<PREFIX-TO-MATCH/MASK>|any]

deny prefix-list <1-4292967294> [<PREFIX-TO-MATCH/MASK> {ge <0-32>|le <0-32>}|
any]
```

Parameters

```
• deny prefix-list <1-4292967294> [<PREFIX-TO-MATCH/MASK> {ge <0-32>|le <0-32>}|
any]
```

deny prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]	Creates and configures a deny prefix-list rule • <1-4294967295> – Configures a sequence number for this deny rule. Specify a value from 1 - 4294967295. Within a prefix list, rules are applied in an ascending order of their sequence number. Rules with lower sequence number are applied first. • <PREFIX-TO-MATCH/MASK> – Specify the prefix to match. For example 10.0.0.0/8 or 192.168.13.0/24. Routes matching the specified prefix are filtered. • ge <0-32> – Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask) • le <0-32> – Optional. Specifies a less than or equal to value for the IP prefix length The 'ge' and 'le' options specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria. • any – Sets the prefix match criteria to *any*. When selected, all routes are filtered, and the action applied is deny. At the backend, this option sets the match criteria to *0.0.0.0/0 le 32*.

Example

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#deny prefix-list 1 168.192.13.0/24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

Related Commands

no	Removes a deny prefix-list rule from this IP prefix list

28.1.2 permit

bgp-ip-prefix-list-config commands

Creates and configures a permit prefix-list rule. The permit rule specifies match criteria based on which prefixes received from (or transmitted to) a BGP neighbor are filtered. A permit action is applied on these filtered prefixes. For example, in the BGP router neighbor context a filter is applied using a IP prefix list. The list contains a permit rule with a prefix to match as 172.168.10.0/24. All prefixes received from the neighbor matching this prefix are permitted.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
permit prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]
```

Parameters

- `permit prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]`

deny prefix-list <1-4294967295> [<PREFIX-TO-MATCH/MASK>|any]	Creates and configures a permit prefix-list rule • <1-4294967295> – Configures a sequence number for this permit rule. Specify a value from 1 - 4294967295. Within a prefix list, rules are applied in an ascending order of their sequence number. Rules with lower sequence number are applied first. • <PREFIX-TO-MATCH/MASK> – Specify the prefix to match. For example 10.0.0.0/8 or 192.168.13.0/24. Routes matching the specified prefix are filtered. • ge – Optional. Specifies a greater than or equal to value for the IP prefix length (subnet mask) • le – Optional. Specifies a less than or equal to value for the IP prefix length Use the 'ge' and 'le' options to specify a IP prefix length range. Use these options to specify a more specific (granular) prefix match criteria. • any – Sets the prefix match criteria to *any*. When selected, all routes are filtered, and the action applied is permit. At the backend, this option sets the match criteria to *0.0.0.0/0 le 32*.

Example

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#permit prefix-list 2 172.122.10.0/
24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
 permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

Related Commands

no	Removes a permit prefix rule from this IP prefix list

28.1.3 no

bgp-ip-prefix-list-config commands

Removes the specified deny or permit prefix-list rule from this IP prefix list

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no [deny|permit]

no [deny|permit] prefix-list <1-4294967295> {<PREFIX-TO-MATCH/MASK>|any}
```

Parameters

- no <PARATMETERS>

no <PARAMETERS>	Removes a deny or permit rule from this IP prefix list

Example

The following example shows the IP prefix list 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
 permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

The following example shows the IP prefix list 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-prefix-list-test)#no deny prefix-list 1 168.192.13.0/
24

nx9500-6C8809(config-bgp-ip-prefix-list-test)#show context
bgp ip-prefix-list test
 permit prefix-list 2 172.122.10.0/24
nx9500-6C8809(config-bgp-ip-prefix-list-test)#
```

28.2 bgp-ip-access-list-config commands

BORDER GATEWAY PROTOCOL

BGP peers and route maps can reference a single IP based *access control list* (ACL). Apply IP ACLs to both inbound and outbound route updates. When applied to a BGP enabled router, every route update is passed through the ACL. Each ACL contains deny and permit entries that are applied sequentially, in the order they appear within the list. When a route matches an entry, the decision to permit or deny the route is applied. Once a match is made the remaining entries in the ACL are not processed.

BGP IP ACLs are used as match criteria in the following contexts:

- BGP neighbor. For more information, see *use*.
- BGP route-map context. For more information, see *match*.

To navigate to the BGP IP ACL configuration instance, use the following command:

```
<DEVICE>(config)#bgp ip-access-list <IP-ACL-NAME>

<DEVICE>(config-bgp-ip-access-list-<IP-ACL-NAME>)#?
BGP IP Access List Mode commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

<DEVICE>(config-bgp-ip-access-list-<IP-ACL-NAME>)#
```

The following table summarizes the BGP IP access list configuration commands:

Table 28.2 *BGP-IP-ACL-Config Commands*

Command	Description	Reference
deny	Creates and configures a deny entry rule for this BGP IP ACL	*page 28-8*
permit	Creates and configures a permit entry for this BGP IP ACL	*page 28-9*
no	Removes a deny or permit entry from this BGP IP ACL	*page 28-10*

28.2.1 deny

bgp-ip-access-list-config commands

Creates and configures a deny entry for this BGP IP ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]
```

Parameters

- `deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]`

deny access-list [<PREFIX-TO-MATCH/MASK> {exact-match}| any]	Creates and configures a deny entry for this BGP IP ACL • <PREFIX-TO-MATCH/MASK> – Specify the prefix to match. • exact-match – Optional. Enables an exact match of the prefix provided in the previous step. When configured, the route is denied only in case of an exact match. • any – Specifies the prefix to match as 'any'.

Example

```
nx9500-6C8809(config-bgp-ip-access-list-test)#deny access-list 192.168.13.0/24
exact-match

nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

Related Commands

no	Removes the specified the deny entry in this IP BGP ACL

28.2.2 permit

bgp-ip-access-list-config commands

Creates and configures a permit entry for this BGP IP ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]
```

Parameters

- `permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]`

permit access-list [<PREFIX-TO-MATCH/MASK> {exact-match}|any]	Creates and configures a permit entry for this BGP IP ACL • <PREFIX-TO-MATCH/MASK> – Specify the prefix to match. • exact-match – Optional. Enables an exact match of the prefix provided in the previous step. When configured, the route is permitted only in case of an exact match. • any – Specifies the prefix to match as 'any'.

Example

```
nx9500-6C8809(config-bgp-ip-access-list-test)#permit access-list 172.168.10.0/24

nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 permit access-list 172.168.10.0/24
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

Related Commands

no	Removes the specified the permit entry in this IP BGP ACL

28.2.3 no

bgp-ip-access-list-config commands

Removes a deny or permit entry from this BGP IP ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no [deny|permit]

no [deny|permit] access-list [<PREFIX-TO-MATCH/MASK>|any]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny or permit entry from this BGP IP ACL

Example

The following example shows the BGP IP ACL 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 permit access-list 172.168.10.0/24
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#

nx9500-6C8809(config-bgp-ip-access-list-test)#no permit access-list 172.168.10.0/
24
```

The following example shows the BGP IP ACL 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-ip-access-list-test)#show context
bgp ip-access-list test
 deny access-list 192.168.13.0/24 exact-match
nx9500-6C8809(config-bgp-ip-access-list-test)#
```

28.3 bgp-as-path-list-config commands

BORDER GATEWAY PROTOCOL

BGP enabled devices use routing updates to exchange network routing information with each other. This information includes route details, such as the network number, path specific attributes, and the list of *Autonomous System Numbers* (ASNs) that a route traverses to reach a destination. This list is contained in the *AS path.*

An AS path *access control list* (ACL) filters AS paths (routes) included in routing updates. Each AS path access list consists of deny and/or permit rules that define regular expressions (match criteria). When configured and applied on inbound and outbound routing updates, the BGP AS path attributes are matched against the regular expressions specified in the AS path ACL. In case of a match, the route is filtered and an action (deny or permit) is applied. Once a match is made subsequent rules in the AS path access list are not processed.

AS path access lists also help prevent looping within an AS. Routing loops are prevented by rejecting routing updates containing local ASNs. Since local ASNs indicate that the route has already traveled through that autonomous system, by rejecting them looping is avoided.

AS path access lists are used as match criteria in the following contexts:

- BGP neighbor. For more information, see *use*.
- BGP route map context. For more information, see *match*.

To navigate to the AS path configuration instance, use the following command:

```
<DEVICE>(config)#bgp as-path <AS-PATH-LIST-NAME>

<DEVICE>(config-bgp-as-path-list-<AS-PATH-LIST-NAME>)#?
BGP AS Path List Mode commands:
  deny      Specify packets to reject
  no        Negate a command or set its defaults
  permit    Specify packets to forward

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

<DEVICE>(config-bgp-as-path-list-<AS-PATH-LIST-NAME>)#
```

The following table summarizes the BGP AS path list configuration commands:

Table 28.3 *BGP-AS-Path-List-Config Commands*

Command	Description	Reference
deny	Creates and configures a deny as-path-list rule	*page 28-12*
permit	Creates and configures a permit as-path-list rule	*page 28-13*
no	Removes a deny or permit rule from this AS path ACL	*page 28-14*

28.3.1 deny

bgp-as-path-list-config commands

Creates and configures a deny as-path-list rule. The deny rule specifies a regular expression to match. This regular expression, a string against the BGP AS paths contained in routing updates. AS paths matching the provided string are filtered and a deny action is applied.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
deny as-path <REG-EXP>
```

Parameters

- `deny as-path <REG-EXP>`

deny as-path <REG-EXP>	Configures a match criteria (regular expression). • <REG-EXP> – Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule) Regular expressions are treated as a 'ASCII string' and not as a sequence of numbers. Create a regular expression ideally suited to filter the required AS paths.

Usage Guidelines

The following table lists some of the characters used in forming regular expressions:

Character to use	Description
^	Indicates the start of a string
$	Indicates the end of a string
_ (underscore)	Indicates a comma, left brace, right brace, start and end of an input string, or a space. For example, "_ _".

Example

```
nx9500-6C8809(config-bgp-as-path-list-test)#deny as-path ^100$

nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
nx9500-6C8809(config-bgp-as-path-list-test)#
```

Related Commands

no	Removes the specified deny as-path ACL rule

28.3.2 permit

bgp-as-path-list-config commands

Creates and configures a permit as-path-list rule. The permit rule specifies a regular expression to match. This regular expression is matched against the BGP AS paths contained in routing updates. AS paths matching the provided string are filtered and a permit action is applied.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
permit as-path <REG-EXP>
```

Parameters

- `permit as-path <REG-EXP>`

permit as-path <REG-EXP>	Configures a match criteria (regular expression). • <REG-EXP> – Specify the regular expression to match (should not exceed 64 characters and should be unique to the AS path list rule) Regular expressions are treated as a 'ASCII string' and not as a sequence of numbers. Create a regular expression which is ideally suited to filter the required AS paths.

Usage Guidelines

The following table lists some of the characters used in forming regular expressions:

Character to use	Description
^	Indicates the start of a string
$	Indicates the end of a string
_ (underscore)	Indicates a comma, left brace, right brace, start and end of an input string, or a space. For example, "_ _".

Example

```
nx9500-6C8809(config-bgp-as-path-list-test)#permit as-path _200_

nx9500-6C8809(config-bgp-as-path-list-test)#permit as-path _323_

nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
 permit as-path _323_
 permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
```

Related Commands

no	Removes the specified permit as-path ACL rule

28.3.3 no

bgp-as-path-list-config commands

Removes a deny or permit rule from this AS path ACL

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no as-path-list [deny|permit] <REG-EXP>
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes a deny or permit rule from this AS path ACL

Example

```
nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
 permit as-path _323_
 permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#

nx9500-6C8809(config-bgp-as-path-list-test)#no permit as-path _323_

nx9500-6C8809(config-bgp-as-path-list-test)#show context
bgp as-path-list test
 deny as-path ^100$
 permit as-path _200_
nx9500-6C8809(config-bgp-as-path-list-test)#
```

28.4 bgp-community-list-config commands

BORDER GATEWAY PROTOCOL

Creates and configures a named community list

IP BGP routes have a set of attributes, mandatory and optional. The community and extended community attributes are optional. Optional attributes are specified by network administrators to mark (color) routes received in updates containing these attributes. These marked routes are filtered and special actions applied (accepted, preferred, distributed, or advertised). For example, the NO_EXPORT community, indicates that routes attached to it are local and not to be advertised to external ASs. Similarly, a set of routes using a common routing policy can be tagged to a community, and the policy applied to the community.

A BGP community is a group of routes sharing common attributes. Route updates contain community information in the form of path attributes. These attributes help identify community members.

A BGP community list is a list of deny or permit entries. It is either assigned a name (regular expressions, predefined community names) or a number. Assigning names to communities increases the number of configurable community lists. All rules applicable to numbered communities apply to named communities too. The only difference being in the number of attributes configurable for a named community list.

Since the community attribute is optional, it is shared only between devices that understand communities and are configured to handle communities. By default the community attribute is not sent to neighbors unless the send-community command option is enabled in the BGP neighbor context. For more information, see *send-community*.

Some of the predefined, globally used communities are:

- no-export – Routes tagged to this community are not advertised to external BGP peers
- no-advertise – Routes tagged to this community are not advertised to any BGP peers
- local-as – Routes tagged to this community are not advertised outside the local AS
- internet – Routes tagged to this community are advertised to the internet community. By default all BGP enabled devices belong to this community.

BGP community lists are used in the following context as match clauses:

- BGP route map context. For more information, see *match*.

To navigate to the BGP community configuration instance, use the following command:

```
<DEVICE>(config)#bgp community-list <COMMUNITY-LIST-NAME>

<DEVICE>(config-bgp-community-list-<COMMUNITY-LIST-NAME>)#?
BGP Community List Mode commands:
  deny      Add a BGP Community List deny rule to Specify community to reject
  no        Negate a command or set its defaults
  permit    Add a BGP Community List permit rule to Specify community to accept

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
```

```
  show      Show running system information
  write     Write running configuration to memory or terminal

<DEVICE>(config-bgp-community-list-<COMMUNITY-LIST-NAME>)#
```

The following table summarizes the BGP community list configuration commands:

Table 28.4 *BGP-Community-List-Config Commands*

Command	Description	Reference
deny	Creates and configures a deny community (expanded or standard) rule	*page 28-17*
permit	Creates and configures a permit community (expanded or standard) rule	*page 28-19*
no	Removes an existing deny or permit community rule from this community list	*page 28-21*

28.4.1 deny

bgp-community-list-config commands

Creates and configures a deny community (expanded or standard) rule

Standard community lists specify known communities and community numbers. Expanded community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
deny community [expanded|standard]

deny community expanded <LINE>

deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

- `deny community expanded <LINE>`

deny community expanded <LINE>	Configures a deny expanded community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the community attributes. • <LINE> – Provide the regular expression.

- `deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]`

deny community standard [AA:NN|internet|local-AS|no-advertise|no-export]	Configures a deny standard community list entry and associates it with a predefined, globally used, known community or community number. The options are: • aa:nn - Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number. • internet – Advertises this route to the internet community • local-AS – Prevents transmission of this route outside the local AS • no-advertise – Prevents advertisement of this route to any peer (internal or external • no-export – Prevents advertisement of this route to external BGP peers (keeping this route within an AS)

Example

```
nx9500-6C8809(config-bgp-community-list-test)#deny community expanded 100

nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
 deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#

nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 5.9.0.0-029R
!
!
version 2.5
!
!
.....................................................
!
bgp ip-prefix-list PrefixList_01
 deny prefix-list 1 192.163.0.0/16 ge 17 le 17
!
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
 permit prefix-list 2 172.122.10.0/24
!
bgp community-list test
 deny community expanded 100
!
--More--
nx9500-6C8809(config)#
```

Related Commands

no	Removes the specified deny community rule from this community list

28.4.2 permit

bgp-community-list-config commands

Creates and configures a permit community (expanded or standard) rule

Standard community lists specify known communities and community numbers. Expanded community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
permit community [expanded|standard]

permit community expanded <LINE>

permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

- `permit community expanded <LINE>`

permit community expanded <LINE>	Configures a permit expanded community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the community attributes. • <LINE> – Provide the regular expression.

- `permit community standard [AA:NN|internet|local-AS|no-advertise|no-export]`

permit community standard [AA:NN|internet| local-AS| no-advertise| no-export]	Configures a permit standard community list entry and associates it with a predefined, globally used, known community or community number. The options are: • aa:nn – Configures the community number. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number. • internet – Advertises this route to the internet community • local-AS – Prevents transmission of this route outside the local AS • no-advertise – Prevents advertisement of this route to any peer (internal or external • no-export – Prevents advertisement of this route to external BGP peers (keeping this route within an AS)

Example

```
nx9500-6C8809(config-bgp-community-list-test)#permit community expanded 300

nx9500-6C8809(config-bgp-community-list-test)# show context
bgp community-list test
 permit community expanded 300
 deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#

nx9500-6C8809(config-bgp-community-list-test1)#permit community standard no-
export

nx9500-6C8809(config-bgp-community-list-test1)#show context
bgp community-list test1
 permit community standard no-export
nx9500-6C8809(config-bgp-community-list-test1)#
```

```
nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 5.9.1.0-026R
!
version 2.5
!
!
.....................................................
!
bgp ip-prefix-list PrefixList_01
 deny prefix-list 1 192.163.0.0/16 ge 17 le 17
!
bgp ip-prefix-list test
 deny prefix-list 1 168.192.13.0/24
 permit prefix-list 2 172.122.10.0/24
!
bgp community-list test
 permit community expanded 300
 deny community expanded 100
!
bgp community-list test1
 permit community standard no-export
!
--More--
nx9500-6C8809(config)#
```

Related Commands

no	Removes the specified permit community rule from this community list

28.4.3 no

bgp-community-list-config commands

Removes a deny or permit community rule from this community list

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no [deny|permit] community expanded <LINE>

no [deny|permit] community standard [AA:NN|internet|local-AS|no-advertise|no-
export]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes a deny or permit expanded community rule from this community list • <LINE> – Specify the regular expression associated with the rule.

Example

The following example shows the settings of the community list 'test' before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
 permit community expanded 300
 deny community expanded 100
nx9500-6C8809(config-bgp-community-list-test)#

nx9500-6C8809(config-bgp-community-list-test)#no deny community expanded 100
```

The following example shows the settings of the community list 'test' after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-community-list-test)#show context
bgp community-list test
 permit community expanded 300
nx9500-6C8809(config-bgp-community-list-test)#
```

28.5 bgp-extcommunity-list-config commands

BORDER GATEWAY PROTOCOL

Creates an configures a named extended community list

A BGP extended community is a group of routes sharing a common attribute, regardless of their network or physical boundary. By using a BGP extended community attribute, routing policies can implement inbound or outbound route filters based on the extended community tag, rather than a long list of individual permit or deny rules. A BGP extended community list is used to create groups of communities to use in a match clause of a route map. An extended community list is used to control which routes are accepted, preferred, distributed, or advertised.

The BGP extended community and standard community attributes are identical in function and structure, except that the former is an eight octet and the latter is a four octet attribute.

BGP extended community lists are used as match clauses in the following context:

- BGP route map context. For more information, see *match*.

To navigate to the extended community configuration instance, use the following command:

```
<DEVICE>(config)#bgp extcommunity-list <EXTCOMMUNITY-LIST-NAME>

<DEVICE>(config-bgp-extcommunity-list-<EXTCOMMUNITY-LIST-NAME>)#?
BGP Extcommunity List Mode commands:
  deny      Add a BGP Community List deny rule to specify extcommunity to
            reject
  no        Negate a command or set its defaults
  permit    Add a BGP Community List permit rule to specify extcommunity to
            accept

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

<DEVICE>(config-bgp-excommunity-list-<EXTCOMMUNITY-LIST-NAME>)#
```

The following table summarizes the BGP extended community list configuration commands:

Table 28.5 *BGP-Extcommunity-List-Config Commands*

Command	Description	Reference
deny	Creates and configures a deny extended community (expanded or standard) rule	*page 28-23*
permit	Creates and configures a permit extended community (expanded or standard) rule	*page 28-25*
no	Removes an existing deny or permit extended community rule from this extcommunity list	*page 28-27*

28.5.1 deny

bgp-extcommunity-list-config commands

Creates and configures a deny extended community (expanded or standard) rule

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
deny extcommunity [expanded|standard]

deny extcommunity expanded <LINE>

deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

Parameters

- `deny extcommunity expanded <LINE>`

deny extcommunity expanded <LINE>	Configures a deny expanded named extended community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the extended community attributes. • <LINE> – Provide the regular expression.

- `deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>`

deny extcommunity standard [rt|soo] <COMMUNITY-NUMBER>	Configures a deny standard named extended community list entry. and associates it with the target or origin community attributes. • rt – Configures the *route target* (RT) extended community attribute • soo – Configures the *site-of-origin* (SOO) extended community attribute • <COMMUNITY-NUMBER> – Specify the community number in one of the following formats: *AA:NN* or *A.B.C.D:NN*

Example

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#deny extcommunity standard rt
200:12

nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#

nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 5.9.1.0-026R
!
!
version 2.5
!
.................................................
!
bgp community-list test1
 permit community standard no-export
!
bgp extcommunity-list test
 deny extcommunity standard rt 200:12
!
--More--
nx9500-6C8809(config)#
```

Related Commands

no	Removes the specified deny extended community rule from this extcommunity list

28.5.2 permit

bgp-extcommunity-list-config commands

Creates and configures a permit extended community (expanded or standard) rule

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
permit extcommunity [expanded|standard]

permit extcommunity expanded <LINE>

permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

Parameters

- `permit extcommunity expanded <LINE>`

permit extcommunity expanded <LINE>	Configures a permit expanded named extended community list entry and associates it with a regular expression to match. The regular expression represents the patterns to match in the extended community attributes. • <LINE> – Provide the regular expression.

- `permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER>`

permit extcommunity standard [rt|soo] <COMMUNITY-NUMBER>	Configures a permit standard named extended community list entry. and associates it with the target or origin community attributes. • rt – Configures the RT extended community attribute • soo – Configures the SOO extended community attribute • <COMMUNITY-NUMBER> – Specify the community number in one of the following formats: *AA:NN* or *A.B.C.D:NN*

Example

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#permit extcommunity standard rt
192.168.13.13:12

nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 permit extcommunity standard rt 192.168.13.13:12
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#

nx9500-6C8809(config)#show context
!
! Configuration of NX9500 version 5.9.1.0-026R
!
!
version 2.5
!
.....................................................
!
bgp community-list test1
 permit community standard no-export
!
bgp extcommunity-list test
 permit extcommunity standard rt 192.168.13.13:12
 deny extcommunity standard rt 200:12
!
```

```
--More--
nx9500-6C8809(config)#
```

Related Commands

no	Removes the specified permit extended community rule from this extcommunity list

28.5.3 no

bgp-extcommunity-list-config commands

Removes an existing deny or permit extended community rule from this extcommunity list

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no [deny|permit] extcommunity expanded <LINE>

no [deny|permit] extcommunity standard [rt|soo] <COMMUNITY-NUMBER>
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes a deny or permit expanded extended community rule from this community list

Example

The following example shows the extended community 'test' settings before the 'no' command is executed:

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 permit extcommunity standard rt 192.168.13.13:12
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#

nx9500-6C8809(config-bgp-extcommunity-list-test)#no permit extcommunity standard
192.168.13.13:12
```

The following example shows the extended community 'test' settings after the 'no' command is executed:

```
nx9500-6C8809(config-bgp-extcommunity-list-test)#show context
bgp extcommunity-list test
 deny extcommunity standard rt 200:12
nx9500-6C8809(config-bgp-extcommunity-list-test)#
```

28.6 bgp-route-map-config commands

BORDER GATEWAY PROTOCOL

BGP route maps are used to control and modify routing information. A BGP route map is a collection of deny and/or permit route rules that define and control redistribution of routes between routers and routing processes. Each rule consists of match criteria and set lines. If a route matches a criteria, the corresponding set line is applied, and the route is passed to the BGP table or to the neighbor, depending on whether the route map is set for incoming or outgoing route updates.

Use the (config) instance to configure BGP route map related parameters.

To navigate to this instance, use the following command:

```
<DEVICE>(config)#route-map <ROUTE-MAP-NAME>

<DEVICE>(config)#route-map test
<DEVICE>(config-dr-route-map-test)#?
Route Map Mode commands:
  deny      Add a deny route map rule to deny set operations
  no        Negate a command or set its defaults
  permit    Add a permit route map rule to permit set operations

  clrscr    Clears the display screen
  commit    Commit all changes made in this session
  do        Run commands from Exec mode
  end       End current mode and change to EXEC mode
  exit      End current mode and down to previous mode
  help      Description of the interactive help system
  revert    Revert changes
  service   Service Commands
  show      Show running system information
  write     Write running configuration to memory or terminal

<DEVICE>(config-dr-route-map-test)#

In the route-map configuration mode, use the following commands to create and
configure a deny or permit route map rule:

<DEVICE>(config-dr-route-map-test)#deny route-map <1-65535>
<DEVICE>(config-dr-route-map-test)#permit route-map <1-65535>

For example:
<DEVICE>(config-dr-route-map-test)#permit route-map 1
<DEVICE>(config-dr-route-map-test)#deny route-map 2

<DEVICE>(config-dr-route-map-test)#show context
route-map test
 permit route-map 1
 deny route-map 2
<DEVICE>(config-dr-route-map-test)#
```

```
<DEVICE>(config-dr-route-map-test-dr-route-map-rule-1)#?
Route Map Rule Mode commands:
  description  Configure comment for this route map
  match        Match values from routing table
  no           Negate a command or set its defaults
  set          Set values in destination routing protocol

  clrscr       Clears the display screen
  commit       Commit all changes made in this session
  do           Run commands from Exec mode
  end          End current mode and change to EXEC mode
  exit         End current mode and down to previous mode
  help         Description of the interactive help system
  revert       Revert changes
  service      Service Commands
  show         Show running system information
  write        Write running configuration to memory or terminal

<DEVICE>(config-dr-route-map-test-dr-route-map-rule-1)#
```

The following table summarizes BGP deny/permit route map rules configuration mode commands:

Table 28.6 *BGP-Route-Map-Config-Mode Commands*

Command	Description	Reference
description	Configures a description for this route-map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions	*page 28-30*
match	Configures the match criteria associated with this deny or permit BGP route map	*page 28-31*
no	Removes or reverts the settings defined for a deny or permit route-map rule	*page 28-34*
set	Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules	*page 28-35*

28.6.1 description

bgp-route-map-config commands

Configures a description for this route map rule (deny or permit) that uniquely distinguishes it from others with similar access permissions

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
description <LINE>
```

Parameters

- `description <LINE>`

description <LINE>	Provide a description for the route map rule (should not exceed 64 characters in length)

Example

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#description "This is
 a deny route map rule"

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
 deny route-map 1
  description "This is a deny route map rule"
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

Related Commands

no	Removes this deny/permit route-map rule's description

28.6.2 match

bgp-route-map-config commands

Configures the match criteria associated with this deny or permit BGP route map

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
match [as-path|community|extcommunity|ip-address|ip-next-hop|ip-route-source|
metric|origin|tag]

match [as-path <AS-PATH-LIST-NAME>|community <COMMUNITY-LIST-NAME> {exact-
match}|extcommunity <EXTCOMMUNITY-LIST-NAME>]

match [ip-address|ip-next-hop|ip-route-source] [BGP-IP-ACCESS-LIST <BGP-ACL-
NAME>|prefix-list <PREFIX-LIST-NAME>]

match metric <0-4294967295>

match origin [egp|igp|incomplete]

match tag <0-65535>
```

Parameters

- `match [as-path <AS-PATH-LIST-NAME>|community <COMMUNITY-LIST-NAME> {exact-match}|extcommunity <EXTCOMMUNITY-LIST-NAME>]`

as-path <AS-PATH-LIST-NAME>	Configures a BGP AS path list to match An AS path is a list of ASs a packet traverses to reach its destination. • <AS-PATH-LIST-NAME> – Specify the AS path list name (should be existing and configured)
community <COMMUNITY-LIST-NAME> {exact-match}	Configures the AS community list string to match • <COMMUNITY-LIST-NAME> – Specify the AS community list name (should be existing and configured). • exact-match – Optional. Does an exact match when matching the specified AS community string. This option is disabled by default.
extcommunity <EXTCOMMUNITY-LIST-NAME>	Configures the external community list string to match • <EXTCOMMUNITY-LIST-NAME> – Specify the external community list name (should be existing and configured).

- `match [ip-address|ip-next-hop|ip-route-source] [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>|prefix-list <PREFIX-LIST-NAME>]`

match	Configures match criteria used to filter BGP routes when forwarding packets
ip-address [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>| prefix-list <PREFIX-LIST-NAME>]	Configures a string of IP addresses, in the route, to match The *IP Address* is a list of IP addresses in the route used to filter the route. Use one of the following options to provide a list of IP addresses: • BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured). • prefix-list <PREFIX-LIST-NAME> – Associates an existing IP address prefix list with this BGP route map. The *IP Address Prefix List* is a list of prefixes in the route used to filter route. Specify the prefix list name (should be existing and configured).

ip-next-hop [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>| prefix-list <PREFIX-LIST-NAME>]	Configures the next-hop's IP address to match The *IP Next Hop* is a list of IP addresses used to filter routes based on the IP address of the next-hop in the route. Use one of the following options to provide next-hop's IP addresses: • BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured). • prefix-list <PREFIX-LIST-NAME> – Associates an existing IP next-hop prefix list with this BGP route map. The *IP Next Hop Prefix List* is a list of prefixes for the route's next-hop determining how the route is filtered. Specify the prefix list name (should be existing and configured).
ip-route-source [BGP-IP-ACCESS-LIST <BGP-ACL-NAME>| prefix-list <PREFIX-LIST-NAME>]	Configures the advertised route source IP address to match The *IP Route Source* is a list of IP addresses used to filter routes based on the advertised IP address of the source. Use one of the following options to provide route-source IP addresses: • BGP-IP-ACCESS-LIST <BGP-ACL-NAME> – Associates an existing BGP ACL with this BGP route map. Specify the BGP ACL name (should be existing and configured). • prefix-list <PREFIX-LIST-NAME> – Associates an existing IP route source prefix list with this BGP route map. The *IP Route Source Prefix List* is a list of prefixes used to filter routes based on the prefix list used for the source. Specify the prefix list name (should be existing and configured).

- `match metric <0-4294967295>`

match metric <0-4294967295>	Defines the exterior metric, used for route map distribution, to match BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost. • <0-4294967295> – Specify the external metric value from 0 - 4294967295.

- `match origin [egp|igp|incomplete]`

match origin [gp|igp|incomplete]	Configures the source of the BGP route to match. Options include: • egp – Matches if the origin of the route is from the *exterior gateway protocol* (eBGP). eBGP exchanges routing table information between hosts outside an autonomous system. • igp – Matches if the origin of the route is from the *interior gateway protocol* (iBGP). iBGP exchanges routing table information between routers within an autonomous system. • incomplete – Matches if the origin of the route is not identifiable

- `match tag <0-65535>`

match tag <0-65535>	Configures the BGP route tag to match The *Tag* is a way to preserve a route's AS path information for routers in iBGP. This option is disabled by default. • <0-65535> – Specify the iBGP route's tag from 0 - 65535.

Example

The following examples show the configuration of match criteria for the deny route-map rule 1:

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#match as-path Filter
List_01

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#match ip-route-source
prefix-list PrefixList_01

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
 deny route-map 1
  description "This is a deny route map rule"
  match as-path FilterList_01
  match ip-route-source prefix-list PrefixList_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

A permit route-map rule 2 is added to the BGP route-map “test”.

```
nx9500-6C8809(config-dr-route-map-test)#permit route-map 2
```

A match criteria is added for the permit route-map rule 2.

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#match ip-next-hop
DL_01

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#show context
 permit route-map 2
  match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-2)#
```

The following example displays the BGP route-map “test” settings:

```
nx9500-6C8809(config-dr-route-map-test)#show context
route-map test
 deny route-map 1
  description "This is a deny route map rule"
  match as-path FilterList_01
  match ip-route-source prefix-list PrefixList_01
 permit route-map 2
  match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test)#
```

Related Commands

no	Removes match criteria associated with a deny or permit route-map rule

28.6.3 no

bgp-route-map-config commands

Removes or reverts the settings defined for a deny or permit route-map rule

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no [description|match <PARAMETERS>|set <PARAMETERS>]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes the description configured for a deny or permit route-map rule

Example

The following example shows the 'deny route-map rule-1' settings before the 'no' commands are executed:

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
 deny route-map 1
  description "This is a deny route map rule"
  match as-path FilterList_01
  match ip-route-source prefix-list PrefixList_01
  set aggregator-as 1 192.168.13.7
  set as-path exclude 20
  set ip next-hop peer-address
  set metric 300
  set local-preference 30
  set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no match as-path
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no set aggregator-as
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#no set metric
```

The following example shows the 'deny route-map rule-1' settings after the 'no' commands are executed:

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
 deny route-map 1
  description "This is a deny route map rule"
  match ip-route-source prefix-list PrefixList_01
  set as-path exclude 20
  set ip next-hop peer-address
  set local-preference 30
  set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

The following example shows the route-map 'test' settings:

```
nx9500-6C8809(config-dr-route-map-test)#show context
route-map test
 deny route-map 1
  description "This is a deny route map rule"
  match ip-route-source prefix-list PrefixList_01
  set as-path exclude 20
  set ip next-hop peer-address
  set local-preference 30
  set community internet
 permit route-map 2
  match ip-next-hop DL_01
nx9500-6C8809(config-dr-route-map-test)#
```

28.6.4 set

bgp-route-map-config commands

Configures the values attributed to a route matching the match criteria specified in the BGP deny or permit route-map rules. These attributes are applied before the route is sent out.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
set [aggregator-as|as-path|atomic-aggregate|comm-list|community|extcommunity|ip|
local-preference|metric|origin|originator-id|source-ip|tag|weight]

set aggregator-as <1-4294967295> <IP>

set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}

set atomic-aggregate

set comm-list delete <COMMUNITY-LIST-NAME>

set community [<COMMUNITY-NUMBER>|none]

set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>

set ip next-hop [<IP>|peer-address]

set local-preference <0-4294967295>

set metric <0-4294967295>

set origin [egp|igp|incomplete]

set originatorid <IP>

set source-ip <IP>

set tag <0-65535>

set weight <0-4294967295>
```

Parameters

- `set aggregator-as <1-4294967295> <IP>`

set aggregator-as <1-4294967295> <IP>	Configures the BGP aggregator's ASN and IP address. Aggregates minimize the size of routing tables. Aggregation combines the characteristics of multiple routes and advertises them as a single route. The configured BGP aggregator settings are applied to filtered routes. • <1-4294967295> – Specify the route aggregator's ASN from 1- 4294967295. This option is disabled by default. • <IP> – Specify the route aggregator's IP address. BGP allows the aggregation of specific routes into one route using an aggregate IP address.

- `set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}`

set as-path [exclude|prepend] <1-4294967295> {<1-4294967295>}	Configures the BGP transform AS path attribute to be applied to filtered routes • exclude – Configures a single AS, or a list of ASs, excluded from the AS path • prepend – Configures a single AS, or a list of ASs, prepended to the AS path • <1-4294967295> – This keyword is common to the 'exclude' and 'prepend' parameters. Use it to specify the AS number. The ASs identified here are excluded or prepended depending on the option selected. You can configure multiple ASNs.

- `set atomic-aggregate`

set atomic-aggregate	Enables BGP atomic aggregate attributes When a BGP enabled wireless controller or service platform receives a set of overlapping routes from a peer, or if the set of routes selects a less specific route, then the local device must set this value when propagating the route to its neighbors. This option is disabled by default.

- `set comm-list delete <COMMUNITY-LIST-NAME>`

set comm-list delete <COMMUNITY-LIST-NAME>	Deletes specified BGP communities. All communities matching the community list name string are deleted from the route. A BGP community is a group of routes sharing a common attribute. • <COMMUNITY-LIST-NAME> – Specify the community list name.

- `set community [<COMMUNITY-NUMBER>|none]`

set community [<COMMUNITY-NUMBER>|none]	Configures a community attribute for this route • <COMMUNITY-NUMBER> – Specify a community attribute. Use one of the following formats: • internet - Advertises this route to the Internet. This is a global community. • local-AS - Prevents the transmit of packets outside the local AS • no-advertise - Prevents advertisement of this route to any peer, either internal or external • no-export - Prevents advertisement of this route to BGP peers, keeping this route within an AS. • aa:nn - Configures the first part (aa) representing the AS number. The second part (nn) represents a 2-byte number. • none – Specifies community attribute as *none*

- `set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>`

set extcommunity [rt|soo] <EXTCOMMUNITY-NUMBER>	Configures a extended community attribute for this route • rt – Identifies the *route target* (rt) extended community • soo – Identifies the *site-of-origin* (soo) community. This is the origin community associated with the route reflector. • <EXTCOMMUNITY-NUMBER> – This keyword is common to the 'rt' and 'soo' parameters. Use it to specify the extended community number.

- `set ip next-hop [<IP>|peer-address]`

set ip next-hop [<IP>|peer-address]	Configures the next hop for this route. Use one of the following options to identify the next hop: • <IP> – Specify the nest hop's IP address • peer-address – Enables the identification of the next-hop address for peer devices. This option is disabled by default

- `set local-preference <0-4294967295>`

set local-preference <0-4294967295>	Configures the BGP local preference path attribute for this route map. When configured, enables the communication of preferred routes out of the AS between peers. This option is disabled by default • <0-4294967295> – Specify the preference value from 0 - 4294967295.

- `set metric <0-4294967295>`

set metric <0-4294967295>	Configures a metric for the route BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost. • <0-4294967295> – Specify the metric from 0 - 4294967295.

- `set origin [egp|igp|incomplete]`

set origin [egp|igp|incomplete]	Configures the origin code for this BGP route map • egp - Sets the origin of the route to eBGP • igp - Sets the origin of the route to iBGP • incomplete - Sets the origin of the route as not identifiable. Use this option if the route is from a source other than eBGP or iBGP.

- `set originatorid <IP>`

set originatorid <IP>	Configures this route map's originator IP address

- `set source-ip <IP>`

set source-ip <IP>	Configures this route map's source IP address • <IP> – Specify the IP address in the A.B.C.D format.

- `set tag <0-65535>`

set tag <0-65535>	Configures this route map's tag value The Tag is a way to preserve a route's AS path information for routers in iBGP. • <0-65335> – Specify a tag value from 0 - 65535.

- `set weight <0-4294967295>`

set weight <0-4294967295>	Enables assignment of a weighted priority to the aggregate route • <0-4292967295> – Specify a value from 0 - 4294967295.

Example

```
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set aggregator-as 1
192.168.13.7

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set as-path exclude
20

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set community
internet

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set ip next-hop peer-
address

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set local-preference
30

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#set metric 300

nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#show context
 deny route-map 1
  description "This is a deny route map rule"
  match as-path FilterList_01
  match ip-route-source prefix-list PrefixList_01
  set aggregator-as 1 192.168.13.7
  set as-path exclude 20
  set ip next-hop peer-address
  set metric 300
  set local-preference 30
  set community internet
nx9500-6C8809(config-dr-route-map-test-dr-route-map-rule-1)#
```

Related Commands

no	Removes the attributes configured for this route map

28.7 bgp-router-config commands

BORDER GATEWAY PROTOCOL

Use the (device-config) or (profile-config) instance to configure BGP router related parameters.

To navigate to the BGP router configuration instance, in the device-config mode, use the following commands:

```
<DEVICE>(config)#self
<DEVICE>(config-device-<MAC>)#router bgp
<DEVICE>config-device <MAC>-router-bgp)#

<DEVICE>config-device <MAC>-router-bgp)#?
Router BGP Mode commands:
  aggregate-address   Configure aggregate address
  asn                 Configure local Autonomous System Number
  bgp                 Border Gateway Protocol
  bgp-route-limit     Limit for number of routes handled by BGP process
  distance            Configure administrative distance
  ip                  Internet Protocol (IP)
  network             Configure a local network
  no                  Negate a command or set its defaults
  route-redistribute  Redistribute information from another routing protocol
  timers              Adjust routing timers

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
  end                 End current mode and change to EXEC mode
  exit                End current mode and down to previous mode
  help                Description of the interactive help system
  revert              Revert changes
  service             Service Commands
  show                Show running system information
  write               Write running configuration to memory or terminal

<DEVICE>config-device <MAC>-router-bgp)#
```

When configured as a profile, the router settings are applied to all devices using the profile.

To navigate to the BGP router configuration instance, in the profile-config mode, use the following commands:

```
<DEVICE>(config)#profile <DEVICE-TYPE> <PROFILE-NAME>

<DEVICE>(config-profile-<PROFILE-NAME>)#router bgp
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#

<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#?
Router BGP Mode commands:
  aggregate-address   Configure aggregate address
  asn                 Configure local Autonomous System Number
  bgp                 Border Gateway Protocol
  bgp-route-limit     Limit for number of routes handled by BGP process
  distance            Configure administrative distance
  ip                  Internet Protocol (IP)
  network             Configure a local network
  no                  Negate a command or set its defaults
  route-redistribute  Redistribute information from another routing protocol
  timers              Adjust routing timers

  clrscr              Clears the display screen
  commit              Commit all changes made in this session
  do                  Run commands from Exec mode
```

```
  end                  End current mode and change to EXEC mode
  exit                 End current mode and down to previous mode
  help                 Description of the interactive help system
  revert               Revert changes
  service              Service Commands
  show                 Show running system information
  write                Write running configuration to memory or terminal

<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#
```

The following table summarizes BGP router configuration mode commands:

Table 28.7 *BGP-Router-Config-Mode Commands*

Command	Description	Reference
aggregate-address	Creates and configures an aggregate address entry in the BGP database	*page 28-41*
asn	Configures this BGP router's ASN	*page 28-42*
bgp	Configures BGP router parameters	*page 28-43*
bgp-route-limit	Configures the BGP route limit parameters	*page 28-48*
distance	Configures administrative distance parameters	*page 28-49*
ip	Configures the BGP default gateway's priority	*page 28-50*
network	Configures the local network IP addresses and masks	*page 28-51*
no	Removes the BGP router settings	*page 28-52*
route-redistribute	Enables redistribution of routes learnt from other routing protocols into BGP	*page 28-53*
timers	Enables adjustment of keepalive and holdtime intervals	*page 28-55*

28.7.1 aggregate-address

bgp-router-config commands

Creates and configures an aggregate address entry in the BGP database

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
aggregate-address <IP/M> {as-set {summary-only}|summary-only}
```

Parameters

- `aggregate-address <IP/M> {as-set {summary-only}|summary-only}`

aggregate-address <IP/M>	Specify the aggregate IP address and mask
as-set {summary-only}	Optional. Summarizes the AS_PATH attributes of the individual routes aggregated • summary-only – Optional. Filters more specific routes from updates

Example

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#aggregate-address
192.168.13.10/32 as-set summary-only

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 192.168.13.10/32 as-set summary-only
   bgp neighbor 192.168.13.199
   remote-as 1
   use route-map UnSupMap_01 in
  bgp neighbor 192.168.13.99
   remote-as 199
   timers connect 10
   timers 20 40
   maximum-prefix 9999 80 restart 50
  bgp neighbor 1.1.1.1
   remote-as 2
   timers connect 10
   timers 20 40
   maximum-prefix 1000000
  bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#
```

Related Commands

no	Removes the aggregate address entry

28.7.2 asn

bgp-router-config commands

Configures the ASN. The ASN represents a group of routers under the same administration and using IGP and common metrics to define how to route packets. In short the ASN represents all routers within an AS.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
asn <1-4294967295>
```

Parameters

- `asn <1-4294967295>`

asn <1-4294967295>	Specify the ASN from 1 - 4294967295.

Example

```
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#asn 1

nx9500-6C8809(config-profile NX9500Profile-router-bgp)#show context
 router bgp
  asn 1
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#
```

28.7.3 bgp

bgp-router-config commands

Configures BGP router parameters

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
bgp [always-compare-med|bestpath|client-to-client|cluster-id|confederation|
dampening|default|deterministic-med|enable|enforce-first-as|fast-external-
failover|graceful-restart|log-neighbor-changes|neighbor|network|router-id|scan-
time]

bgp [always-compare-med|deterministic-med|enable|enforce-first-as|fast-external-
failover|log-neighbor-changes]

bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-
worst}|missing-as-worst}]
bgp client-to-client reflection
bgp cluster <IP>
bgp confederation [identifier|peers] <1-4294967295>
bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255>
bgp default [ipv4-unicast|local-preference <0-4294967295>]
bgp graceful-restart {stalepath-time <1-3600>}
bgp neighbor <IP>
bgp network import-check
bgp router-id <IP>
bgp scan-time <5-60>
```

Parameters

```
• bgp [always-compare-med|deterministic-med|enable|enforce-first-as|fast-
external-failover|log-neighbor-changes]
```

always-compare-med	Enables comparison of *Multi-exit Discriminators* (MEDs) received from neighbors. This option is disabled by default. MED is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared when selecting the best route to the host network. A route with a lower MED value is preferred over a route with a higher MED value. BGP does not discriminate between iBGP and eBGP when using MED for route selection. This option is mutually exclusive to the *deterministic-med* option.
deterministic-med	Enables selection of the best MED path from amongst all paths advertised by neighboring ASs. This option is disabled by default. MED is used by BGP peers to select the best route among multiple routes. When enabled, MED route values (from the same AS) are compared to select the best route. This best route is then compared with other routes in the BGP route table to select the best overall route. This option is mutually exclusive to the *always-compare-med* option.
enable	Starts the BGP daemon on the device (wireless controller or service platform). BGP is disabled by default.
enforce-first-as	Enforces the first AS for all BGP routes. This option is disabled by default. When enforced, devices deny updates received from an external neighbor that does not have the neighbor's configured AS at the beginning of the received AS path parameter. This enhances security by not allowing traffic from an unauthorized AS.

fast-external-failover	Enables immediate resetting of BGP session on the interface once the BGP connection goes down. This option is enabled by default. When enabled, a session is reset as soon as the direct link to an external peer goes down. Normally, when a BGP connection goes down, the device waits for the expiry of the duration specified in *holdtime* parameter before bringing down the interface. To configure the 'holdtime', use the *timers > bgp > <keepalive-time> > <holdtime>* command in this (BGP router) configuration mode.
log-neighbor-changes	Enables logging of a BGP neighbor's status change (active or not active) events. It also enables the logging of the reason for such change in status.

- `bgp best-path [as-path [confed|ignore]|compare-router-id|med {confed {missing-as-worst}|missing-as-worst}]`

best-path	Modifies the bestpath selection algorithm. The route selection algorithm uses the following criteria when selecting the preferred route: as-path, router-id, and med.
as-path [confed|ignore]	Enables an AS path from being considered as a criteria for selecting the preferred route • confed – Enables comparison of path lengths (including confederation sets and sequences) when selecting a route (EXPERIMENTAL). This option is disabled by default. • ignores – Disables an AS path length from being considered as a criteria for selecting a preferred route. When, disabled the AS path length is ignored. This option is disabled by default.
compare-router-id	Enables the use of router ID as a selection criteria when selecting the preferred route. When enabled, the router ID is used to select the best path between two identical BGP routes. The route with the lower router ID is selected over a route with a higher router ID. This option is disabled by default.
med {confed {missing-as-worst}| missing-as-worst}	Enables comparison of AS path MED value when selecting the preferred route MED is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared to determine the best route to the host network. A route with a lower MED value is preferred over a route with a higher MED value. • confed – Optional. Enables comparison of MED value among confederation paths (EXPERIMENTAL). When enabled, you can optionally enable the treatment of AS paths without the MED value as the least preferable route. This option is disabled by default. • missing-as-worst – Optional. Enables the treatment of AS paths without the MED value as the least preferable route. This option is disabled by default.

- `bgp client-to-client reflection`

client-to-client reflection	Enables client-to-client route reflection (EXPERIMENTAL) Route reflectors are used when all iBGP speakers are not fully meshed. If the clients are fully meshed, the route-reflectors are not required. This option is enabled by default.

- `bgp cluster <IP>`

cluster <IP>	Enables and sets a cluster ID, in case the BGP cluster has more than one route-reflector A cluster generally consists of a single route-reflector and its clients. The cluster is usually identified by the router ID of this single route-reflector. Sometimes, to increase redundancy, a cluster might have more than one route-reflector configured. In this case, all route-reflectors in the cluster are identified by the cluster ID (configured in the IP format).

- `bgp confederation [identifier|peers] <1-4294967295>`

confederation [identifier|peers] <1-4294967295>	Configures AS confederation (group of ASs) parameters (identifier and peers) • identifier – Enables and sets a BGP confederation identifier to allow an AS to be divided into several ASs. In other words an AS is divided into multiple ASs, and together they form a confederation. This confederation is visible to external routers as a single AS. The ASN is usually the confederation ID. Specify a value from 1 - 4294967295. Forming AS confederation reduces iBGP mesh inside an AS. • peers – Configures the maximum number of the ASs constituting this BGP confederation. Specify the AS number from 1 - 4294967295. Multiple ASs can be added to the list of confederation members.

- `bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255>`

bgp dampening {<1-45>} {<1-20000>} <1-20000> <1-255>	Enables dampening and configures dampening parameters. This option is disabled by default. Dampening minimizes the instability caused by route flapping. A penalty is added for every flap in the flapping route. As soon as the total penalty reaches the specified *Route Suppress Limit* value, the advertisement of this route is suppressed. This penalty is delayed when the time specified in *Half Lifetime* occurs. Once the penalty becomes lower than the value specified in *Start Route Reuse*, the advertisement of the route is un-suppressed. • <1-45> – Optional. Configures the half lifetime (in minutes). A penalty is imposed on a route that flaps. This is the time for the penalty to decrease to half its current value. Specify a value from 1 - 45 minutes. The default is 1 minute. • <1-20000> – Optional. Configures the route reuse value. When the penalty for a suppressed route decays below the value specified here, the route is un-suppressed (reused). Specify a value from 1 - 20000. • <1-20000> – Configures the route suppress value. When a route flaps, a penalty is added to the route. When the penalty reaches or exceeds the value specified as the 'maximum duration to suppress a stable route'. Specify a value from 1 - 20000. The maximum duration to suppress a stable route, is the next set of value configured in this command from 1 - 255. • <1-255> – Configures the maximum duration, in minutes, a suppressed route is suppressed. This is the maximum duration for which a route remains suppressed before it is reused. Specify a value from 1 - 255 minutes.

- `bgp default [ipv4-unicast|local-preference <0-4294967295>]`

default	Configures the following defaults for BGP neighbor-related parameters: IPv4 unicast and local preference

ipv4-unicast	Enable IPv4 unicast traffic for neighbors. This option is enabled by default.
local-preference <0-4294967295>	Configures a local preference for the neighbor. Higher the value higher is the preference. • <0-4294967295> – Specify a value from 10 - 4294967295.

- `bgp graceful-restart {stalepath-time <1-3600>}`

default graceful-restart {stalepath-time <1-3600>}	Enables graceful restart on this BGP router. This option is disabled by default • stalepath-time <1-3600> – Optional. Configures the maximum time, in seconds, to retain stale paths from restarting neighbor. This is the time the paths from a restarting neighbor are preserved. All stale paths, unless reinstated by the neighbor after re-establishment, are deleted at the expiry of the time specified here. • <1-3600> – Specify a value from 1 - 3600 seconds.

- `bgp neighbor <IP>`

neighbor <IP>	Configures the BGP neighbor's IP address and enters its configuration mode. Use this command to configure a BGP neighbor's parameters. • <IP> – Specify the IP address in the A.B.C.D format. For BGP neighbor configuration parameters, see *bgp-neighbor-config commands*.

- `bgp network import-check`

network import-check	Enables checking of the existence of BGP network route in IGP before importing

- `bgp router-id <IP>`

router <IP>	Enables the device (BGP supported wireless controller or service platform) identified by the <IP> parameter as a router. The router's IP address is configured as its ID, and uniquely identifies it. When not specified, the IP address of the interface is configured as the router ID. This option is disabled by default.

- `bgp scan-time <5-60>`

scan-time <5-60>	Configures the scanning interval, in seconds, for updating BGP routes. This is the interval between two consecutive scans the BGP device performs in order to validate routes in its routing table. To disable scanning, set the value to Zero (0). • <5-60> – Specify a value from 5 - 60 seconds. The default is 60 seconds.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#bgp router-id 192.168.13.13

nx9500-6C8809(config-profile testNX9000-router-bgp)#aggregate-address
116.117.118.0/24 as-set summary-only

nx9500-6C8809(config-profile testNX9000-router-bgp)#bgp neighbor 192.168.13.99

nx9500-6C8809(config-profile testNX9000-router-bgpp)#show context
 router bgp
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp router-id 192.168.13.13
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
nx9500-6C8809(config-profile testNX9000-router-bgp)#
```

Related Commands

no	Removes the BGP router parameters. The *no > bgp > enable* command disabled BGP.

28.7.4 bgp-route-limit

bgp-router-config commands

Configures the BGP route limit parameters

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
bgp-route-limit [num-routes <VALUE>|reset-time <1-86400>|retry-count <1-32>|
retry-timeout <1-3600>]
```

Parameters

```
• bgp-route-limit [num-routes <VALUE>|reset-time <1-86400>|retry-count <1-32>|
retry-timeout <1-3600>]
```

num-routes <VALUE>	Configures the number of routes that can be stored on this BGP router. Set this value based on the available memory on this BGP router (wireless controller or service platform). • <VALUE> – Specify a value from 1 - 4,294,967,295. The default is 9216 routes.
reset-time <1-86400>	Configures the reset time in seconds. This is the time after which the *retry count* value is set to Zero (0). • <1-86400> – Specify a value from 1- 86,400 seconds. The default is 360 seconds.
retry-count <1-32>	Configures the maximum number of times the BGP process is reset before being permanently shut down. Once shut down, the BGP process has to be started manually. The BGP process is reset if it is flooded with route entries that exceed the maximum number of routes configured for this device. • <1-32> – Specify a value from 1 - 32. The default is 5 routes.
retry-timeout <1-3600>	Configures the duration, in seconds, the BGP process is temporarily shut down, before a reset of the process is attempted. • <1-3600> – Specify a value from 1 - 3600 seconds. The default is 60 seconds.

Example

```
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#bgp-route-limit num-routes
10

nx9500-6C8809(config-profile NX9500Profile-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
  bgp-route-limit num-routes 10
nx9500-6C8809(config-profile NX9500Profile-router-bgp)#
```

Related Commands

no	Removes BGP route limitations configured. Use the no command to revert back to default.

28.7.5 distance

bgp-router-config commands

Configures administrative distance parameters. The distance parameter is a rating of the trustworthiness of a route. The higher the distance, lower is the trust rating. The distance can be set for each type of route indicating its trust rating.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
distance [<IP/M> <1-255> <BGP-ACL-NAME>|bgp <1-255> <1-255> <1-255>]
```

Parameters

- `distance [<IP/M> <1-255> <BGP-ACL-NAME>|bgp <1-255> <1-255> <1-255>]`

distance <IP/M> <1-255> <BGP-ACL-NAME>	Configures the default administrative distance, specified by the <1-255> parameter, when the route's source IP address matches the specified IP prefix- • <IP/M> – Specify the IP source prefix and prefix length. • <1-255> – Specify the distance from 1 - 255. • <BGP-ACL-NAME> – Optional. Specify the BGP access list name.
bgp <1-255> <1-255> <1-255>	Configures the default administrative distance for different route types • <1-255> – Configures the default administrative distance for routes external to this AS. Specify a value from 1 - 255. • <1-255> – Configures the default administrative distance for routes internal to this AS. Specify a value from 1 - 255. • <1-255> – Configures the default administrative distance for local routes. Specify a value from 1 - 255.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#distance bgp 200 100 200

nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  distance bgp 200 100 200
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
  bgp-route-limit num-routes 10
nx9500-6C8809(config-profile testNX9000-router-bgp)#
```

Related Commands

no	Removes the administrative distance related configurations

28.7.6 ip

bgp-router-config commands

Configures the BGP default gateway's priority

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
ip default-gateway priority <1-8000>
```

Parameters

- `ip default-gateway priority <1-8000>`

default-gateway priority <1-8000>	Configures the default gateway's (acquired through BGP) priority • <1-8000> – Specify a value from 1 - 8000. The default is 7500. Lower the value, higher is the priority.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#ip default-gateway priority 1

nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  ip default-gateway priority 1
  bgp-route-limit num-routes 10
nx9500-6C8809(config-profile testNX9000-router-bgpp)#
```

Related Commands

no	Removes the BGP default gateway configuration

28.7.7 network

bgp-router-config commands

Configures the local network IP addresses and masks. These network addresses are broadcasted to neighboring BGP peers. You can configure a single IP address or a range of IP addresses in the A.B.C.D/M notation.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
network <IP/M> {backdoor|pathlimit|route-map}

network <IP/M> {backdoor pathlimit <1-255>
network <IP/M> {pathlimit <1-255>}
network <IP/M> {route-map <ROUTE-MAP-NAME>}
```

Parameters

```
• network <IP/M> {backdoor pathlimit <1-255>|pathlimit <1-255>|route-map <ROUTE-MAP-NAME>}
```

network <IP/M>	Configures the local network's address in the A.B.C.D/M format • <IP/M> – Specify the network address.
backdoor pathlimit <1-255>	Optional. Configures a BGP backdoor route. After configuring the backdoor route, you can optionally configure the as-path hop count limit attribute for this backdoor route. • pathlimit <1-255> – Specify the hop count limit from 1 - 255.
pathlimit <1-255>	Optional. Configures the maximum path limit for this AS • <1-255> – Specify the hop count limit from 1 - 255.
route-map <ROUTE-MAP-NAME>	Optional. Associates a BGP route map with this local network. When applied, the route-map values take precedence • <ROUTE-MAP-NAME> – Specify the route map name.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp)#network 192.168.13.0/24
backdoor pathlimit 200

nx9500-6C8809(config-profile testNX9000-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  distance bgp 200 100 200
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
  network 1.2.3.0/24
  network 192.168.13.0/24 backdoor pathlimit 200
  bgp-route-limit num-routes 10
nx9500-6C8809(config-profile testNX9000-router-bgp)#
```

Related Commands

no	Removes the list of local networks configured

28.7.8 no

bgp-router-config commands

Removes the BGP router settings

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no [aggregate-address|bgp|bgp-route-limit|distance|ip|network|route-redistribute|
   timers]
```

Parameters

- no <PARAMETERS>

no <PARAMETERS>	Removes the BGP router settings

Example

The following example shows the BGP router settings before the 'no' commands have been executed:

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.199
   remote-as 1
   use route-map UnSupMap_01 in
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
  bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no bgp neighbor
192.168.13.99
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no aggregate-address
116.117.118.0/24
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#no bgp-route-limit
```

The following example shows the BGP router settings after the 'no' commands have been executed:

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  bgp neighbor 192.168.13.199
   remote-as 1
   use route-map UnSupMap_01 in
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#
```

28.7.9 route-redistribute

bgp-router-config commands

Enables redistribution of routes learnt from other routing protocols into BGP

Large ISP networks using multiple routing protocols, need to enable redistribution of routes across routing protocols. Routing protocols differ in their basic characteristics, such as metrics, administrative distance, classful and classless capabilities, etc. When enabling redistribution, these differences have to be taken into consideration.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
route-redistribute [connected|kernel|ospf|static] {metric <0-4294967295>|route-map <ROUTE-MAP-NAME>}
```

Parameters

```
• route-redistribute [connected|kernel|ospf|static] {metric <0-4294967295>|route-map <ROUTE-MAP-NAME>}
```

route-redistribute	Redistributes routes learnt from other protocols
connected	Redistributes directly connected routes • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see *match*.
kernel	Redistributes kernel routes. These are routes that are neither connected, nor static, nor dynamic. • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see *match*.
ospf	Redistributes OSPF routes • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see *match*.
static	Redistributes static routes • metric <0-4294967295> – Optional. Specify the metric for the redistributed routes. • route-map <ROUTE-MAP-NAME> – Optional. Specifies the route map name. The route map defines the match criteria based on which routes are filtered before redistribution. For more information on route maps, see *match*.

Example

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#route-redistribute
connected metric 200

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
  bgp neighbor 192.168.13.199
   remote-as 1
   use route-map UnSupMap_01 in
  route-redistribute connected metric 200
  bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#
```

Related Commands

no	Disables redistribution of routes learnt from other routing protocols into BGP

28.7.10 timers

bgp-router-config commands

Enables adjustment of keepalive and holdtime intervals

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
timers bgp <0-65535> <0-65535>
```

Parameters

- `timers bgp <0-65535> <0-65535>`

timers bgp <0-65535> <0-65535>	Configures the keepalive and holdtime interval in seconds • <0-65535> – Specify a keepalive interval from 0 - 65535 seconds. It is the interval, in seconds, between two successive keepalive packets exchanged with this router and its neighbor to keep the TCP connection alive. • <0-65535> – Specify a holdtime value from 0 - 65535 seconds. This is the time this router will wait without receiving a keepalive packet from its neighbor before declaring it dead. If the time since the last keepalive packet received (from its neighbor) exceeds the value set here, the neighbor is declared dead.

Example

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#timers bgp 100 100

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#show context
 router bgp
  bgp enable
  asn 1
  aggregate-address 116.117.118.0/24 as-set summary-only
  bgp neighbor 192.168.13.199
   remote-as 1
   use route-map UnSupMap_01 in
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
  timers bgp 100 100
  bgp-route-limit num-routes 10 reset-time 360
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp)#
```

Related Commands

no	Reverts BGP timers to default

28.8 bgp-neighbor-config commands

BORDER GATEWAY PROTOCOL

BGP enabled devices connected through an established TCP connection are referred to as BGP peers or neighbors. To establish a TCP connection, BGP routers exchange open messages containing the following information: AS number, BGP version running, BGP router ID, and timer values (keepalive and holdtime). Once these values are accepted by both devices, the connection is established and the routers become neighbors. With the TCP connection established the BGP neighbors begin sharing routing information and updates. A failure in the establishment of the TCP connection indicates that the routers are not neighbors and cannot exchange routing information.

Use the (profile/device-config) instance to configure BGP neighbors.

To navigate to the BGP neighbor configuration instance, use the following commands:

```
<DEVICE>(config)#profile <PROFILE-NAME>

<DEVICE>(config-profile <PROFILE-NAME>)#router bgp
<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#?

<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#bgp neighbor ?
  A.B.C.D  IP address of the bgp neighbor

<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#

<DEVICE>(config-profile <PROFILE-NAME>-router-bgp)#bgp neighbor <IP>
<DEVICE>(config-profile <PROFILE-NAME>-router--bgp-neighbor-<IP>)#?
Router BGP Neighbor Mode commands:
  activate                    Enable the Address Family for this Neighbor
                              (EXPERIMENTAL)
  advertisement-interval      Minimum interval between BGP routing updates
  allowas-in                  Accept as-path with my AS present in it
                              (EXPERIMENTAL)
  attribute-unchanged         BGP attribute is propagated unchanged to this
                              neighbor (EXPERIMENTAL)
  capability                  Advertise capability to the peer
  default-originate           Originate default route to this neighbor
  description                 Neighbor specific description
  disable-connected-check     One-hop away EBGP peer using loopback address
                              (EXPERIMENTAL)
  dont-capability-negotiate   Do not perform capability negotiation
                              (EXPERIMENTAL)
  ebgp-multihop               Allow EBGP neighbors not on directly connected
                              networks
  enforce-multihop            Enforce EBGP neighbors perform multihop
                              (EXPERIMENTAL)
  local-as                    Specify a local-as number (EXPERIMENTAL)
  maximum-prefix              Maximum number of prefix accept from this peer
  next-hop-self               Disable the next hop calculation for this
                              neighbor
  no                          Negate a command or set its defaults
  override-capability         Override capability negotiation result
  passive                     Don't send open messages to this neighbor
  password                    Set a password
  peer-group                  Set peer-group for this neighbor (EXPERIMENTAL)
  port                        Neighbor's BGP port (EXPERIMENTAL)
  remote-as                   Specify a BGP neighbor
  remove-private-as           Remove private AS number from outbound updates
                              (EXPERIMENTAL)
  route-server-client         Configure a neighbor as Route Server client
                              (EXPERIMENTAL)
  send-community              Send Community attribute to this neighbor
```

```
shutdown                    Administratively shut down this neighbor
soft-reconfiguration        Per neighbor soft reconfiguration
strict-capability-match     Strict capability negotiation match
                            (EXPERIMENTAL)
timers                      BGP per neighbor timers
unsuppress-map              Route-map to selectively unsuppress suppressed
                            routes
update-source               Source of routing updates
use                         Set setting to use
weight                      Set default weight for routes from this neighbor

clrscr                      Clears the display screen
commit                      Commit all changes made in this session
do                          Run commands from Exec mode
end                         End current mode and change to EXEC mode
exit                        End current mode and down to previous mode
help                        Description of the interactive help system
revert                      Revert changes
service                     Service Commands
show                        Show running system information
write                       Write running configuration to memory or terminal
```

```
<DEVICE>(config-profile <PROFILE-NAME>-router--bgp-neighbor-<IP>)#
```

The following table summarizes BGP deny/permit route map rules configuration mode commands:

Table 28.8 *BGP-Neighbor-Config-Mode Commands*

Command	Description	Reference
activate	Enables an address family for this neighbor (EXPERIMENTAL)	*page 28-59*
advertisement-interval	Configures the minimum interval between two consecutive BGP router updates	*page 28-60*
allowas-in	Enables re-advertisement of all prefixes containing duplicate ASNs (EXPERIMENTAL)	*page 28-61*
attribute-unchanged	Enables the propagation of BGP attribute values unchanged to this neighbor BGP device (EXPERIMENTAL)	*page 28-62*
capability	Enables the advertisement of capability (dynamic and ORF) to BGP peers	*page 28-63*
default-originate	Enables the sending of the default route to BGP neighbors. It also allows the configuration of the default route.	*page 28-64*
description	Configures a description for a BGP neighbor device	*page 28-65*
disable-connected-check	Enables one-hop away EBGP peer using loop back address (EXPERIMENTAL)	*page 28-66*
dont-capability-negotiate	Disables capability negotiation with BGP neighbors (EXPERIMENTAL)	*page 28-67*
ebgp-multihop	Enables *eBGP Multihop* on this BGP neighbor, and configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other.	*page 28-68*
enforce-multihop	Forces EBGP neighbors to perform multi-hop checks (EXPERIMENTAL)	*page 28-69*
local-as	Configures this neighbor's local AS number. Also enables the prepending of this AS number in route updates. (EXPERIMENTAL)	*page 28-70*
maximum-prefix	Configures the maximum number of prefixes that can be received from a BGP neighbor	*page 28-71*
next-hop-self	Enables next-hop calculation for this neighbor	*page 28-72*

Table 28.8 *BGP-Neighbor-Config-Mode Commands*

Command	Description	Reference
no	Removes this BGP neighbor's settings, or reverts them back to default	*page 28-73*
override-capability	Enables the overriding of capability negotiation results	*page 28-74*
passive	Enables this BGP neighbor device (or devices using this profile) as passive	*page 28-75*
password	Sets a password for this BGP neighbor device (or devices using this profile)	*page 28-76*
peer-group	Sets the peer group for this BGP neighbor device (or devices using this profile) (EXPERIMENTAL)	*page 28-77*
port	Configures a non-standard BGP port for this BGP neighbor (EXPERIMENTAL)	*page 28-78*
remote-as	Configures the ASN for this neighbor BGP device (or devices using this profile)	*page 28-79*
remove-private-as	Removes the private ASN from outbound updates (EXPERIMENTAL)	*page 28-80*
route-server-client	Enables this BGP neighbor device (or devices using this profile) to act as a route server client (EXPERIMENTAL)	*page 28-81*
send-community	Enables sending of the community attribute to the BGP neighbor	*page 28-82*
shutdown	Shuts down this BGP neighbor device (or devices using this profile)	*page 28-83*
soft-reconfiguration	Enables storing of updates for inbound soft reconfiguration	*page 28-84*
strict-capability-match	Enables a strict capability match before allowing a neighbor BGP peer to open a connection (EXPERIMENTAL)	*page 28-85*
timers	Configures this BGP neighbor's keepalive and holdtime durations	*page 28-86*
unsuppress-map	Uses a route-map that selectively un suppresses routes that have been suppressed using the *aggregate-address* command	*page 28-88*
update-source	Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor	*page 28-89*
use	Configures filters for this neighbor. These filters are BGP IP ACL, IP prefix list, AS path list, and route map. Based on the filters used, updates received from this neighbor are filtered.	*page 28-90*
weight	Configures a weight for all routes learned from this BGP neighbor	*page 28-91*

28.8.1 activate

bgp-neighbor-config commands

Enables an address family for this neighbor. This option is enabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
activate
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9500-router-bgp-neighbor-
192.168.13.99)#activate
```

28.8.2 advertisement-interval

bgp-neighbor-config commands

Configures the minimum interval, in seconds, between two consecutive BGP router updates

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
advertisement-interval <0-600>
```

Parameters

- `advertisement-interval <0-600>`

advertisement-interval <0-600>	Configures the minimum interval, in seconds, between two consecutive BGP router updates. Sending too many router updates creates flapping of routes leading to possible disruptions. Specify a minimum interval so that the BGP routing updates are sent after the set interval. • <0-600> – Specify a value from 0 - 600 seconds. The default is 5 seconds.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
advertisement-interval 100

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Reverts the advertisement interval to default (5 seconds)

28.8.3 allowas-in

bgp-neighbor-config commands

Enables re-advertisement of all prefixes containing duplicate ASNs. Use this command to configure the maximum number of times an ASN is advertised. This option is disabled by default.

When enabled, *Provider Edge* (PE) routers can re-advertise all prefixes containing duplicate ASNs. This creates a pair of *VPN Routing/Forwarding* (VRF) instances on each PE router to receive and re-advertise prefixes. The PE router receives prefixes with ASNs from all PE routers and advertises to its neighbor PE routers on one VRF. The other VRF receives prefixes with ASNs from the *Customer Edge* (CE) routers and re-advertises them to all PE routers in the configuration.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
allowas-in <1-10>
```

Parameters

- `allowas-in <1-10>`

allowas-in <1-10>	Enables and configures the maximum number of times an ASN is advertised. • <1-10> – Specify a value from 1 - 10.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
allowas-in 10

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables re-advertisement of all prefixes containing duplicate ASNs

28.8.4 attribute-unchanged

bgp-neighbor-config commands

Enables propagation of BGP attribute values unchanged to this neighbor BGP device. The BGP attributes are: as-path, med, and next-hop.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
attribute-unchanged {(as-path|med|next-hop)}
```

Parameters

- `attribute-unchanged {(as-path|med|next-hop)}`

attribute-unchanged	Enables the propagation of the following BGP attribute values unchanged: • as-path – Optional. Enables propagation of AS path BGP attribute unchanged to this neighbor BGP device. This option is disabled by default. • med – Optional. Enables propagation of MED BGP attribute unchanged to this neighbor BGP device. This option is disabled by default • next-hop – Optional. Enables propagation of the next-hop BGP attribute value unchanged to this neighbor BGP device. This option is disabled by default.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
attribute-unchanged as-path

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables propagation of BGP attribute values unchanged to this neighbor BGP device

28.8.5 capability

bgp-neighbor-config commands

Enables the advertisement of capability (dynamic and ORF) to BGP peers

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
capability [dynamic|orf]

capability dynamic
capability orf prefix-list [both|receive|send]
```

Parameters

- `capability dynamic`

capability dynamic	Enables the advertisement of dynamic capability Enable this option to show a neighbor device's capability to advertise or withdraw and address capability to other peers in a non-disruptive manner. This option is disabled by default.

- `capability orf prefix-list [both|receive|send]`

capability dynamic [both|receive|send]	Enables the advertisement of *Outbound Router Filtering* (ORF) capability. This option is disabled by default. Enable this option to enable ORF, and advertise this capability to peer devices. ORFs send and receive capabilities to lessen the number of updates exchanged between BGP peers. By filtering updates, ORF minimizes update generation and exchange overhead. The local BGP device advertises ORF in the *send* mode. The peer BGP device receives the ORF capability in the *receive* mode. The two devices exchange updates to maintain the ORF for each router. Only a peer group or an individual BGP router can be configured to be in *receive* or *send* mode. A a peer group member cannot be configured. • both – Advertises the capability to send and receive the ORF to/from this neighbor • receive – Advertises the capability to receive the ORF from this neighbor • send – Advertises the capability to send the ORF to this neighbor

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
capability orf prefix-list both

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables advertisement of capability (dynamic and ORF) to BGP peers

28.8.6 default-originate

bgp-neighbor-config commands

Enables the sending of the default route to BGP neighbors. It also allows the configuration of the default route. When enabled and configured, local BGP routers send the default route 0.0.0.0 (or a route map specified route) to its neighbor for use as the default route.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
default-originate {route-map <BGP-ROUTE-MAP-NAME>}
```

Parameters

- `default-originate {route-map <BGP-ROUTE-MAP-NAME>}`

default-originate {route-map <BGP-ROUTE-MAP-NAME>}	Enables *default originate* on this BGP neighbor. This option is disabled by default. • route-map <BGP-ROUTE-MAP> – Optional. Use this keyword to specify a route map to use as the default originate route If no route-map is specified, the default route 0.0.0.0 is sent.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#default-originate

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables the sending of the default route to BGP neighbors

28.8.7 description

bgp-neighbor-config commands

Configures a description for this BGP neighbor device

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
description neighbor <LINE>
```

Parameters

- `description neighbor <LINE>`

neighbor <LINE>	Specify a description for this BGP neighbor device (should not exceed 80 characters).

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#description neighbor "This neighbor is an external AS neighbor"

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes this BGP neighbor's description

28.8.8 disable-connected-check

bgp-neighbor-config commands

Enables one-hop away eBGP peer using loop back address. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
disable-connected-check
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#disable-connected-check

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables one-hop away eBGP peer using loop back address

28.8.9 dont-capability-negotiate

bgp-neighbor-config commands

Disables capability negotiation with BGP neighbors. This is to allow compatibility with older BGP versions that have no capability parameters used in the *open* messages between peers. Capability negotiation is enabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
dont-capability-negotiate
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
dont-capability-negotiate

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Enables capability negotiation with BGP neighbors

28.8.10 ebgp-multihop

bgp-neighbor-config commands

Enables *eBGP Multihop* on this BGP neighbor. When enabled, allows neighbor connection to be established between two eBGP neighbors that are not directly connected to each other. Use this command to configure the maximum number of hops possible between two such eBGP neighbors. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
ebgp-multihop <1-255>
```

Parameters

- `ebgp-multihop <1-255>`

ebgp-multihop <1-255>	Configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other. • <1-255> – Specify a value from 1 - 255. The default is 255.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#ebgp-
multihop 20

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables eBGP Multihop on this BGP neighbor

28.8.11 enforce-multihop

bgp-neighbor-config commands

Forces eBGP neighbors to perform multi-hop checks

A *multihop* route is a route to external peers on indirectly connected networks. When enforced, eBGP neighbors perform
multi-hop check. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
enforce-multihop
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#enforce-multihop

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables enforcement of multihop route checks

28.8.12 local-as

bgp-neighbor-config commands

Configures this neighbor's local AS number

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
local-as <1-4294967295> {no-prepend}
```

Parameters

- `local-as <1-4294967295> {no-prepend}`

local-as <1-4294967295> {no-prepend}	Configures the local AS number • <1-4292967295> – Specify a value from 1 - 4294967295. • no-prepend – Optional. Select to enable. When enabled, the local AS number is not prepended to route updates from eBGP peers. AS numbers are prepended to route updates by default.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#local-
as 20 no-prepend

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the local AS number. And also reverts prepending of AS numbers to default (allows prepending).

28.8.13 maximum-prefix

bgp-neighbor-config commands

Configures the maximum number of prefixes that can be received from a BGP neighbor. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
maximum-prefix <1-4294967295> {(<1-100>|restart <1-65535>|warning-only)}
```

Parameters

- `maximum-prefix <1-4294967295> {(<1-100>|restart|warning-only)}`

maximum-prefix <1-4294967295>	Configures the maximum number of prefixes that can be received from a BGP neighbor • <1-4294967295> – Specify a value for 1 - 4294967295. • <1-100> – Optional. Sets the threshold limit for generating a log message. This value represents a percentage of the maximum-prefix configured in the preceding step. When this value is reached, a log entry is generated. For example if the maximum-prefix is set to 100 and *threshold limit* is set to 65, then after receiving 65 prefixes, a log entry is generated. This option is disabled by default. • restart <1-65535> – Optional. Restarts BGP peer connection once the maximum-prefix limit specified is exceeded. For example, If the value specified is 10, then after receiving 10 prefixes from the neighbor, the system restarts the connection with that neighbor. Specify a value from 1 - 65535. This option is disabled by default. • warning-only – Configure to enable. When the maximum-prefix limit is exceeded, the connection is restarted. However, when this option is enabled, the connection is not restarted and an event is generated instead. This option is disabled by default.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#maximum-prefix 400 50 warning-only

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
con
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the maximum prefix settings configured for this neighbor

28.8.14 next-hop-self

bgp-neighbor-config commands

Enables next-hop calculation for this neighbor. This option is disabled by default.

When enabled, this device (or devices using this profile) are configured as the next hop for the BGP speaking neighbor or peer group. This allows the BGP device to change the next hop information that is sent to iBGP peers. The next hop address is set to the IP address of the interface used to communicate with the eBGP neighbor.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
next-hop-self
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
next-hop-self

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables next-hop calculation for this neighbor (this is the default)

28.8.15 no

bgp-neighbor-config commands

Removes this BGP neighbor's settings, or reverts them back to default

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
no <PARAMETER>
```

Parameters

- `no <PARAMETER>`

no <PARAMETER>	Specify the parameter details to remove or revert to default

Example

The following example shows the neighbor 192.168.13.99 settings before the 'no' commands are executed:

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no
advertisement-interval
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no
disable-connected-check
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no
default-originate
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#no
local-as

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   description neighbor "This neighbor is an external AS neighbor"
   dont-capability-negotiate
   ebgp-multihop 20
   maximum-prefix 400 50 warning-only
   next-hop-self
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

28.8.16 override-capability

bgp-neighbor-config commands

Enables the overriding of capability negotiation results. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
override-capability
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
override-capability

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables the overriding of capability negotiation results

28.8.17 passive

bgp-neighbor-config commands

Enables this BGP neighbor device (or devices using this profile) as passive. When enabled, local devices do not attempt to open a connection to passive BGP neighbors. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
passive
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#passive

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables this BGP neighbor device (or devices using this profile) as passive

28.8.18 password

bgp-neighbor-config commands

Sets a password for this BGP neighbor device (or devices using this profile). When configured, this password is used for *Message Digest 5* (MD5) authentication between two BGP peers connected over TCP. To enable MD5 authentication between two BGP peers, configure both with the same password.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
password neighbor <LINE>
```

Parameters

- `password neighbor <LINE>`

password neighbor <LINE>	Specify the password.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#password neighbor eBGPneighbor@300

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)# show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the password configured for this neighbor

28.8.19 peer-group

bgp-neighbor-config commands

Sets the peer group for this BGP neighbor device (or devices using this profile). Peer groups are a set of BGP neighbors with the same update policies. This facilitates the updates of various policies, such as, distribute lists and filter lists.

The peer group can be configured as a single entity. Any changes made to the peer group is propagated to all members.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
peer-group <PEER-GROUP-NAME>
```

Parameters

- `peer-group <PEER-GROUP-NAME>`

peer-group <PEER-GROUP-NAME>	Specify the peer group name. Once specified, this neighbor device becomes a member of the peer group identified by the <PEER-GROUP-NAME> keyword. • <PEER-GROUP-NAME> – Specify the peer group name.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#peer-
group eBGPPeerGrp1

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the peer group configuration. This neighbor peer group setting is removed.

28.8.20 port

bgp-neighbor-config commands

Configures a non-standard BGP port for this BGP neighbor

By default BGP uses port 179. Use this command to set a non standard port for this BGP neighbor.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
port <0-65535>
```

Parameters

- `port <0-65535>`

port <0-65535>	Specify a value from 0 - 65535.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#port
21

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the non standard port configured for this neighbor

28.8.21 remote-as

bgp-neighbor-config commands

Configures the ASN for this neighbor BGP device (or devices using this profile). ASN is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
remote-as <1-4294967295>
```

Parameters

- `remote-as <1-4294967295>`

remote-as <1-4294967295>	Specify the remote ASN from 1 - 4294967295.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#remote-as 100

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

28.8.22 remove-private-as

bgp-neighbor-config commands

Removes the private ASN from outbound updates. By default private ASNs are included in outbound updates.

Private AS numbers are not advertised to the Internet. This option is used with external BGP (eBGP) peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
remove-private-as
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
remove-private-as

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
   remove-private-as
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Includes private ASNs in outbound updates (this is the default setting)

28.8.23 route-server-client

bgp-neighbor-config commands

Enables this BGP neighbor device (or devices using this profile) to act as a route server client. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
route-server-client
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
route-server-client

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
   remove-private-as
   route-server-client
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables this BGP neighbor device (or devices using this profile) to act as a route server client

28.8.24 send-community

bgp-neighbor-config commands

Enables sending of the community attribute to the BGP neighbor. The community attribute groups destinations in a certain community and applies routing decisions based on the community. On receiving community attribute, the BGP router announces it to the neighbor.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
send-community [both|extended|standard]
```

Parameters

- `send-community [both|extended|standard]`

send-community [both|extended| standard]	Enables sending of the community attributes to the BGP neighbor • both – Sends extended and standard community attributes • extended – Sends extended community attributes only • standard – Sends standard community attributes only

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
send-community both

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
   remove-private-as
   route-server-client
   send-community both
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Disables sending of the community attribute to the BGP neighbor

28.8.25 shutdown

bgp-neighbor-config commands

Shuts down this BGP neighbor device (or devices using this profile). When configured, this neighbor is administratively shut down. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
shutdown
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-
192.168.13.99)#shutdown

nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remove-private-as
   route-server-client
   shutdown
nx9500-6C8809(config-profile testNX500-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the administrative shut down of this neighbor

28.8.26 soft-reconfiguration

bgp-neighbor-config commands

Enables storing of updates for inbound soft reconfiguration. This option is disabled by default.

Soft-reconfiguration can be used in lieu of BGP route refresh capability. Enabling this option enables local storage of all received routes and their attributes. This requires additional memory on the BGP device.

When a soft reset (inbound) is performed on the neighbor device, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
soft-reconfiguration inbound
```

Parameters

- `soft-reconfiguration inbound`

soft-reconfiguration inbound	Performs a soft reconfiguration (inbound) on the BGP neighbor device

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
soft-reconfiguration inbound
```

Related Commands

no	Disables soft reconfiguration

28.8.27 strict-capability-match

bgp-neighbor-config commands

Enforces a strict capability match before allowing a TCP connection with this neighbor. In case capabilities do not match, the BGP connection is not established. This option is disabled by default.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
strict-capability-match
```

Parameters

None

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#strict-capability-match
```

Related Commands

no	Disables a strict capability match before allowing a connection with this neighbor

28.8.28 timers

bgp-neighbor-config commands

Configures this BGP neighbor's keepalive and holdtime durations

NOTE: The keepalive and holdtime settings configured at the neighbor level override those configured on the BGP router.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
timers [<0-65535> <0-65535>|connect <0-65535>]
```

Parameters

- `timers [<0-65535> <0-65535>|connect <0-65535>]`

timers <0-65535> <0-65535>	Sets the keepalive and holdtime intervals • <0-65535> – Specifies the keepalive interval from 0 - 65535 seconds. It is the interval, in seconds, between two successive keepalive packets exchanged with this neighbor to keep the TCP connection alive. • <0-65535> – Specifies the holdtime interval from 0 - 65535. This is the time this neighbor will wait without receiving a keepalive packet from its neighbor before declaring it dead. If the time since the last keepalive packet received (from its neighbor) exceeds the value set here, the neighbor is declared dead.
timers connect <0-65535>	Sets the BGP connect time. This is the interval, in seconds, after which BGP tries to connect to a dead peer. • <0-65535> – Specify a value from 1 - 65535 seconds.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#timers
20 40

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#timers
connect 20

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   strict-capability-match
   timers connect 20
   timers 20 40
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
```

```
    local-as 20 no-prepend
    maximum-prefix 400 50 warning-only
    next-hop-self
    override-capability
    passive
    password neighbor eBGPneighbor@300
    remove-private-as
    route-server-client
    send-community both
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the holdtime value set for this neighbor

28.8.29 unsuppress-map

bgp-neighbor-config commands

Unsuppresses map to selectively advertise routes that have been suppressed using the *aggregate-address* command

The aggregate-address command creates a route map with a IP/mask address that consolidates subnets under it. This reduces the number of route maps on the BGP device to one consolidated entry. Use unsuppress-map to selectively allow/deny a subnet or a set of subnets from this consolidated entry.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
unsuppress-map <ROUTE-MAP-NAME>
```

Parameters

- `unsuppress-map <ROUTE-MAP-NAME>`

unsuppress-map <ROUTE-MAP-NAME>	Unsuppresses the specified route map • <ROUTE-MAP-NAME> – Specify the route map name.

Example

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#
unsuppress-map test

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-
192.168.13.99#show context
  bgp neighbor 192.168.13.99
   remote-as 199
   maximum-prefix 9999 80 restart 50
   unsuppress-map test
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99#
```

Related Commands

no	Removes the unsuppress flag applied on the specified route map

28.8.30 update-source

bgp-neighbor-config commands

Allows BGP sessions to use any operational interface to establish the TCP connection with this neighbor

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
update-source <IPv4>
```

Parameters

- `update-source <IPv4>`

update-source <IPv4>	Specify the BGP enabled neighbor's IPv4 address.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-
192.168.13.99)#update-source 192.168.13.1

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   strict-capability-match
   timers connect 20
   timers 20 40
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
   remove-private-as
   route-server-client
   send-community both
   update-source 192.168.13.1
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the source of routing updates

28.8.31 use

bgp-neighbor-config commands

Configures filters for this neighbor. These filters are BGP IP ACL, IP prefix list, AS path list, and route map. Based on the filters used, updates received from this neighbor are filtered.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]
```

Parameters

```
• use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]
```

use [distribute-list <BGP-IP-ACL-NAME>|filter-list <AS-PATH-LIST-NAME>|prefix-list <IP-PREFIX-LIST-NAME>|route-map <BGP-ROUTE-MAP-NAME>]	Uses predefined and configured filters with this neighbor
	• distribute-list <BGP-IP-ACL-NAME> – Uses a BGP IP ACL
	  • <BGP-IP-ACL-NAME> – Specify the BGP IP ACL name.
	• filter-list <AS-PATH-LIST-NAME> – Uses an AS path list
	  • <AS-PATH-LIST-NAME> – Specify the AS path list name.
	• prefix-list <IP-PREFIX-LIST-NAME> – Uses a IP prefix list
	  • <IP-PREFIX-LIST-NAME> – Specify the IP prefix list name.
	• route-map <BGP-ROUTE-MAP-NAME> – Uses a route map
	  • <BGP-ROUTE-MAP-NAME> – Specify the route map name.

Example

```
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#use filter-list FilterList_01 in

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#use route-map testBGPRouteMap out

nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#show context
  bgp neighbor 192.168.13.99
   remote-as 199
   use filter-list FilterList_01 in
   maximum-prefix 9999 80 restart 50
   use route-map testBGPRouteMap out
   unsuppress-map test
nx9500-6C8809(config-device B4-C7-99-6C-88-09-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Removes the filters used to filter updates received from this neighbor

28.8.32 weight

bgp-neighbor-config commands

Configures a weight for all routes learned from this BGP neighbor. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The highest weight is always chosen.

Supported in the following platforms:

- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX9500, NX9510, NX9600

Syntax

```
weight <0-65535>
```

Parameters

- `weight <0-65535>`

weight <0-65535>	Specifies a relative weightage for all routes learned from this neighbor • <0-65535> – Specify a value from 0 - 65535.

Example

```
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#weight
10

nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#show
context
  bgp neighbor 192.168.13.99
   remote-as 100
   advertisement-interval 100
   peer-group eBGPPeerGrp1
   port 21
   strict-capability-match
   timers connect 20
   timers 20 40
   allowas-in 10
   attribute-unchanged as-path
   capability orf prefix-list both
   default-originate
   description neighbor "This neighbor is an external AS neighbor"
   disable-connected-check
   dont-capability-negotiate
   ebgp-multihop 20
   enforce-multihop
   local-as 20 no-prepend
   maximum-prefix 400 50 warning-only
   next-hop-self
   override-capability
   passive
   password neighbor eBGPneighbor@300
   remove-private-as
   route-server-client
   send-community both
   update-source 192.168.13.1
   weight 10
nx9500-6C8809(config-profile testNX9000-router-bgp-neighbor-192.168.13.99)#
```

Related Commands

no	Reverts to default value

29 CRYPTO-CMP-POLICY

This chapter summarizes the crypto *certificate management protocol* (CMP) policy commands in the CLI command structure.

CMP is an Internet protocol designed to enable devices (access point, wireless controller, or service platform) to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network. A *Certificate Authority* (CA) issues the certificates using the defined CMP.

WiNG CMP implementation allows you to configure a crypto CMP policy that enables auto installation and auto management of device certificates. When configured and implemented on a device, the crypto CMP policy allows the device to automatically trigger a certification request to a configured, CMP supported CA server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. You can use a manually created trustpoint for one service (like HTTPS) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

Use the (config) instance to configure a crypto CMP policy. To navigate to the crypto CMP policy configuration instance, use the following commands:

```
<DEVICE>(config)#crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
ap6522-D8273A(config)#crypto-cmp-policy CMP
ap6522-D8273A(config-cmp-policy-CMP)#
ap6522-D8273A(config-cmp-policy-CMP)#?
CMP Policy Mode commands:
  ca-server               CMP CA Server configuration commands
  cert-key-size           Set key size for certificate request
  cert-renewal-timeout    Trigger a cert renewal request on timeout
  cross-cert-validate     Validate cross-cert using factory-cert
  no                      Negate a command or set its defaults
  subjectAltName          Configure subjectAltName value
  trustpoint              Trustpoint for CMP
  use                     Set setting to use

  clrscr                  Clears the display screen
  commit                  Commit all changes made in this session
  do                      Run commands from Exec mode
  end                     End current mode and change to EXEC mode
  exit                    End current mode and down to previous mode
  help                    Description of the interactive help system
  revert                  Revert changes
  service                 Service Commands
  show                    Show running system information
  write                   Write running configuration to memory or terminal
ap6522-D8273A(config-cmp-policy-CMP)#
```

This chapter is organized as follows:

- *crypto-cmp-policy-instance*
- *other-cmp-related-commands*

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

29.1 crypto-cmp-policy-instance

- *CRYPTO-CMP-POLICY*

The following table summarizes crypto CMP policy configuration commands:

Table 29.1 *Crypto-CMP-Policy Commands*

Command	Description	Reference
ca-server	Configures the CA server details	*page 29-3*
cert-key-size	Configures the size of the key associated with a certificate request	*page 29-5*
cert-renewal-timeout	Configures a certificate renewal timeout in days	*page 29-6*
cross-cert-validate	Enables validation of the cross certificate with the factory certificate	*page 29-7*
subjectAltName	Configures an alternate subject name for this CMP policy	*page 29-8*
trustpoint	Configures a trustpoint and its associated information, such as the subject name, the sender's (device requesting certification) details, and the recipient's (CA) details	*page 29-9*
use	Associates a device's autogen-uniqueid with this crypto CMP policy	*page 29-11*
no	Removes the crypto CMP policy settings	*page 29-12*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

29.1.1 ca-server

crypto-cmp-policy-instance

Configures the primary and secondary CMP CA server details.

The CA is an external network authority (usually a trusted third-party server) that generates and issues digital certificates in response to requests received from network devices. Use this command to configure the primary and secondary CA server details, such as name of the device hosting the CA server, the port used to access the CA server, and the path where the certificate is stored. Once defined, devices using this CMP policy automatically send requests to the specified primary CA server, and retrieve the certificate from the specified location. If the primary CA server is not reachable, the requests are sent to the secondary CA server.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
ca-server [primary|secondary] host <IP> port <1-65535> path <PATH>
```

Parameters

- `ca-server [primary|secondary] host <IP> port <1-65535> path <PATH>`

ca-server [primary|secondary]	Configures the primary and secondary CMP CA server details (IPv4 address, port, and path) • primary – Configures the primary CMP CA server's details • secondary – Configures the secondary CMP CA server's details The secondary CMP CA is used in case the primary CA server is not reachable. CA server settings are required to complete CMP requests.
host <IP>	Configures IPv4 address of the device hosting the primary/secondary CA server • <IP/HOSTNAME> – Specify the server's IPv4 address.
port <1-65535>	Configures the port on which the primary/secondary CA server can be reached • <1-65535> – Specify the port number from 1 - 65535.
path <PATH>	Configures the path or filename of the primary/secondary CMP CA certificate. Enter the complete relative path to the file on the server. • <PATH> – Specify the path. Once specified, the certificate is downloaded from this location and installed on the device.

Example

```
ap6522-D8273A(config-cmp-policy-CMP)#ca-server primary host 192.168.8.74 port 8
path cmp

ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
ca-server primary host 192.168.8.74 port 80 path cmp
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no	Removes the configured primary/secondary CA server details

29.1.2 cert-key-size

crypto-cmp-policy-instance

Configures the size of the key associated with a certificate request

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
cert-key-size [2048|3072|4096]
```

Parameters

- `cert-key-size [2048|3072|4096]`

cert-key-size [2048|3072|4096]	Configures the certificate request key size. The options are: • 2048 – Sets the key size to 2048 bits. This is the default setting. • 3072 – Sets the key size to 3072 bits • 4096 – Sets the key size to 4096 bits

Example

```
nx9500-6C8809(config-cmp-policy-test)#cert-key-size 3072

nx9500-6C8809(config-cmp-policy-test)#show context
crypto-cmp-policy test
 cert-key-size 3072
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 2
osr2bwjR+0L+G64ny3wfuAAAAAtTFjeFnvOIixTHLDfgt7Bu  reference-id 123456 sender-name
"CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company,
CN=ExampleCompany.com"
nx9500-6C8809(config-cmp-policy-test)#
```

Related Commands

no	Reverts the certificate request key size to default (2048 bits)

29.1.3 cert-renewal-timeout

crypto-cmp-policy-instance

Configures a certificate renewal timeout in days. This is the number of days, before the expiration of the device's certificate, that a certificate renewal is triggered.

The expiration of device's certificate is checked once a day. When a certificate is about to expire a certificate renewal is initiated with the dedicated CMP CA server resource through an existing IPSec tunnel. If the tunnel is not established, the CMP renewal request is not sent. If a renewal succeeds the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
cert-renewal-timeout <1-60>
```

Parameters

- `cert-renewal-timeout <1-60>`

cert-renewal-timeout <1-60>	Configures the certificate renewal timeout in days. This is the number of days, before the expiration of the device's certificate, that a certificate renewal is triggered. Once the configured time is completed, the device triggers a certificate renewal request. • <1-60> – Specify a value from 1 - 60 days. The default is fourteen (14) days. Therefore, by default a device triggers certificate renewal request 14 days before its certificate expires.

Example

```
ap6522-D8273A(config-cmp-policy-CMP)#cert-renewal-timeout 60

ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-renewal-timeout 60
 ca-server primary host 192.168.8.74 port 8 path cmp
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no	Reverts the certificate renewal timeout to default (14 days)

29.1.4 cross-cert-validate

crypto-cmp-policy-instance

Enables validation of the cross certificate using the factory certificate. When enabled, the obtained cross-certificate is validated against the operator's certificate configured using the *trustpoint > cmp-auth-operator* command. An error message is displayed in case the cross-certificate is not obtained or if the cross-certificate is found to be invalid. This option is disabled by default.

NOTE: To the operator certificate, in the device configuration mode execute the *trustpoint > cmp-auth-operator* command. For more information, see *trustpoint (device-config-mode)*.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
cross-cert-validate
```

Parameters

None

Example

```
nx9500-6C8809(config-cmp-policy-test)#cross-cert-validate

nx9500-6C8809(config-cmp-policy-test)#show context
crypto-cmp-policy test
 cert-key-size 3072
 cross-cert-validate
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 2
9piulK/GqvD+G64ny3wfuAAAAAuqCi8WJkNJwryMD9IAPk4T reference-id 123456 sender-name
"CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company,
CN=ExampleCompany.com"
nx9500-6C8809(config-cmp-policy-test)#
```

Related Commands

no	Disables validation of the cross certificate with the factory certificate

29.1.5 subjectAltName

crypto-cmp-policy-instance

Configures the subjectAltName identity for this CMP policy

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn
<FQDN>|string <USER-DEFINED-STRING>]
```

Parameters

```
• subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn
<FQDN>|string <USER-DEFINED-STRING>]
```

subjectAltName [address <IP>|dn <DISTINGUISHED-NAME>|email <EMAIL-ID>|fqdn <FQDN>|string <USER-DEFINED-STRING>]	Configures the subjectAltName identity using one of the following options:
	• address <IP> – Uses IP address as identity
	  • <IP> – Specify the IP address.
	• dn <DISTINGUISHED-NAME> – Uses distinguished name as identity
	  • <DISTINGUISHED-NAME> – Specify the DISTINGUISHED-NAME.
	• email <EMAIL-ID> – Uses e-mail address as identity
	  • <EMAIL-ID> – Specify the e-mail address.
	• fqdn <FQDN> – Uses FQDN as identity
	  • <FQDN> – Specify the FQDN.
	• string <USER-DEFINED-STRING> – Uses a user specified name as identity
	  • <USER-DEFINED-STRING> – Specify the string to use as identity.

Example

```
ap6522-D8273A(config-cmp-policy-CMP)#subjectAltName dn TechPubsCA

ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-update
 cert-renewal-timeout 60
 ca-server primary host 192.168.8.74 port 8 path cmp
 subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no	Removes the subjectAltName identity configured with this CMP policy

29.1.6 trustpoint

crypto-cmp-policy-instance

Configures a trustpoint and its associated information, such as the subject name, the sender's (device requesting certification) details, and the recipient's (CA) details. This information is needed to obtain the certificate from the CA server using CMP.

Each certificate is digitally signed by a *trustpoint* and contains device-specific information, such as device name, IP address, serial number. It helps to uniquely identify a device.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
trustpoint <TRUSTPOINT-NAME> subject-name <WORD> secret [0 <WORD>|2 <WORD>]
reference-id <WORD> sender-name <WORD> [recipient-name <WORD>|ca-psk <CERT-PATH>]
```

Parameters

```
• trustpoint <TRUSTPOINT-NAME> subject-name <WORD> secret [0 <WORD>|2 <WORD>]
reference-id <WORD> sender-name <WORD> [recipient-name <WORD>|ca-psk <CERT-PATH>]
```

trustpoint <TRUSTPOINT-NAME>	Configures a trustpoint name (should not exceed 32 characters) • <TRUSTPOINT-NAME> – Specify the trustpoint's name.
subject-name <WORD>	Configures a subject name for this trustpoint. The subject name should uniquely identify the certificate and should not exceed 512 characters in length.
secret [0 <WORD>|2 <WORD>]	Configures the secret used to encrypt the trustpoint. The secret should not exceed 128 characters in length. • 0 <WORD> – Configures a clear text password • 2 <WORD> – Configures an encrypted password
reference-id <WORD>	Configures the reference ID. The CA server uses this information to identify the shared secret key used. • <WORD> – Specify the reference ID.
sender-name <WORD>	Configures the sender's name. The CA server uses this information to identify the shared secret key used. The sender's name should not exceed 512 characters in length. • <WORD> – Specify the sender name.
recipient-name	Configures the recipient's name. The CA server uses this information to validate the request. The recipient's name should not exceed 256 characters in length.
ca-psk <CERT-PATH>	Configures the certificate path for the server certificate • <CERT-PATH> – Specify the certificate path.

Example

```
ap6522-D8273A(config-cmp-policy-CMP)#trustpoint cmp-test subject-name "CN=Examp
leCompany, O=Example Company" secret 0 test-secret reference-id 123456 sender-na
me "CN=ExampleCompany.com, O=Example Company" recipient-name "O=Example Company,
 CN=ExampleCompany.com"
ap6522-D8273A(config-cmp-policy-CMP)#

ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-update
 cert-renewal-timeout 60
 ca-server primary host 192.168.8.74 port 8 path cmp
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0
test-secret  reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example
Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
 subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no	Removes the trustpoint associated with this crypto CMP policy

29.1.7 use

crypto-cmp-policy-instance

Associates a device's autogen-uniqueid with this crypto CMP policy

A device's autogen-uniqueid is a combination of a user-defined string (prefix or suffix) and a substitution token. The WiNG software implementation provides two built-in substitution tokens: $SN and $MiNT-ID that represent the device's serial number and MiNT ID respectively. These substitution tokens are internally retrieved and combined with the user-defined string to auto generate a unique identity for a device.

To auto generate the device's unique ID, in the device configuration mode execute the following command:

```
autogen-uniqueid <WORD>
```

For more information on the autogen-uniqueid command, see *autogen-uniqueid*.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use autogen-uniqueid
```

Parameters

- `use autogen-uniqueid`

use autogen-uniqueid	Associates a device's autogen-uniqueid with this crypto CMP policy. The device's autogen-uniqueid should be existing and configured.

Example

```
ap6522-D8273A(config-cmp-policy-CMP)#use autogen-uniqueid

ap6522-D8273A(config-cmp-policy-CMP)#show context
crypto-cmp-policy CMP
 cert-update
 cert-renewal-timeout 60
 use autogen-uniqueid
 ca-server primary host 192.168.8.74 port 8 path cmp
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0
test-secret  reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example
Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
 subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#
```

Related Commands

no	Removes the device's autogen-uniqueid associated with this crypto CMP policy

29.1.8 no

crypto-cmp-policy-instance

Removes or reverts this crypto CMP policy settings

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [ca-server <SERVER-NAME>|cert-key-size|cert-renewal-timeout|cross-cert-
validate|subjectAltName|trustpoint <TRUSTPOINT-NAME>|use autogen-uniqueid]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts this crypto CMP policy settings

Example

```
ap6522-D8273A(config-cmp-policy-CMP)#show context
 cert-update
 cert-renewal-timeout 60
 use autogen-uniqueid
 ca-server primary host 192.168.8.74 port 8 path cmp
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0
test-secret  reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example
Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
 subjectAltName dn TechPubsCA
ap6522-D8273A(config-cmp-policy-CMP)#

ap6522-D8273A(config-cmp-policy-CMP)#no cert-renewal-timeout
ap6522-D8273A(config-cmp-policy-CMP)#no subjectAltName

ap6522-D8273A(config-cmp-policy-CMP)#show context
 cert-update
 use autogen-uniqueid
 ca-server primary host 192.168.8.74 port 8 path cmp
 trustpoint cmp-test subject-name "CN=ExampleCompany, O=Example Company" secret 0
test-secret  reference-id 123456 sender-name "CN=ExampleCompany.com, O=Example
Company" recipient-name "O=Example Company, CN=ExampleCompany.com"
ap6522-D8273A(config-cmp-policy-CMP)#
```

29.2 other-cmp-related-commands

- *CRYPTO-CMP-POLICY*

The following table summarizes other commands associated with the implementation of the crypto CMP policy:

Table 29.2 *Other-CMP-Related Commands*

Command	Description	Reference
use	Associates a crypto CMP policy with a device	*page 29-14*
show	Displays current status of CMP requests in progress. This command also displays trustpoint details (CMP and non-CMP trustpoints).	*page 29-15*

29.2.1 use

other-cmp-related-commands

Applies a crypto CMP policy to a device. Once CMP enabled, the device automatically requests for a certificate from the CA server and installs it. After applying the CMP policy, commit and write the change to memory. This is needed to apply this configuration across reboots.

To apply a CMP policy on a device, navigate to the device's config-device mode and execute the *use > crypto-cmp-policy> <CRYPTO-CMP-POLICY-NAME>* command.

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>
```

Parameters

- `use crypto-cmp-policy <CRYPTO-CMP-POLICY-NAME>`

cmp-policy <CRYPTO-CMP-POLICY-NAME>	Applies an existing crypto CMP policy on this device. When associated with a profile, the crypto CMP policy is applied to all devices using the profile. • <CRYPTO-CMP-POLICY-NAME> – Specify the crypto CMP policy name. Should be existing and configured.

Example

```
ap6522-D8273A(config-device-00-11-3F-D8-27-3A)#use crypto-cmp-policy CMP
ap6522-D8273A(config-device-00-11-3F-D8-27-3A)#commit
```

29.2.2 show

other-cmp-related-commands

Displays current status of CMP requests in progress. This command also displays trustpoint details (CMP and non-CMP trustpoints).

Supported in the following platforms:

- Access Points — AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP81XX, AP7602, AP7612, AP7622, AP7632, AP7662, AP82XX, AP8432, AP8533, WiMod
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
show crypto [cmp|pki]

show crypto cmp request status {on <DEVICE-NAME>}
show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}
```

Parameters

- `show crypto cmp request status {on <DEVICE-NAME>}`

show crypto cmp request {on <DEVICE-NAME>}	Displays the current status of all on-going CMP requests • on <DEVICE-NAME> – Optional. Optionally specify the name of the AP, wireless controller, or service platform to view CMP request status on a specified device.

- `show crypto pki trustpoints {<TRUSTPOINT-NAME>|all} {on <DEVICE-NAME>}`

show pki trustpoints {<TRUSTPOINT-NAME>|all} on <DEVICE-NAME>	Displays all trustpoints including CMP generated trustpoints • <TRUSTPOINT-NAME> – Optional. Specify a trustpoint name. Displays details of the trustpoint identified by the <TRUSTPOINT-NAME> parameter. • all – Optional. Displays details of all configured trustpoints • on <DEVICE-NAME> – Optional.Optionally specify the name of the AP, wireless controller, or service platform to view trustpoints configured on a specified device.

Example

```
ap6522-D8273A#show crypto pki trustpoints
-------------------------------------------------------------------------------
-------
    TRUSTPOINT                    KEY NAME                              VALID UNTIL
-------------------------------------------------------------------------------
-------
  cmp-test                          cmp-test-key                       Fri May  9
09:44:22 2014 GMT
  default-trustpoint              default_rsa_key                    Fri Dec 30
00:00:40 2022 GMT
-------------------------------------------------------------------------------
-------

ap6522-D8273A#

ap6522-D8273A(config)#show crypto cmp request status
CMP Request Status:   cmp-complete

ap6522-D8273A#
```

30 ROAMING ASSIST POLICY

This chapter summarizes the Roaming Assist policy commands in the CLI command structure.

By constantly monitoring a client's packets and the *received signal strength indicator* (RSSI) of a given client by a group of access points, decision can be made on the optimal access point to which the client needs to roam. Then forcefully direct the client to the optimal access point.

The threshold intervals are configurable and can be adjusted based on the client load.

Use the (config) instance to configure a Roaming Assist policy. To navigate to the Roaming Assist policy configuration instance, use the following commands:

```
<DEVICE> (config) roaming-assist-policy <ROAMING-ASSIST-POLICY-NAME>

nx9500-6C8809(config)roaming-assist-policy test
nx9500-6C8809(config-roaming-assist-policy-test)#?
Roaming Assist Mode commands:
  action                Configure action - action is deauth / log /
                        assisted-roam
  aggressiveness        Configure the roaming aggressiveness for a wireless
                        client
  detection-threshold   Configure the detection threshold - when exceeded,
                        client monitoring starts
  disassoc-time         Configure the disassociation time - time after which a
                        disassociation is sent
  handoff-count         Configure the handoff count - number of times client
                        can exceed handoff threshold
  handoff-threshold     Configure the handoff threshold - when exceeds an
                        action is taken.
  monitoring-interval   Configure the monitoring interval - interval at which
                        client monitoring occurs
  no                    Negate a command or set its defaults
  sampling-interval     Configure the sampling interval - interval at which
                        client rssi values are checked

  clrscr                Clears the display screen
  commit                Commit all changes made in this session
  end                   End current mode and change to EXEC mode
  exit                  End current mode and down to previous mode
  help                  Description of the interactive help system
  revert                Revert changes
  service               Service Commands
  show                  Show running system information
  write                 Write running configuration to memory or terminal

nx9500-6C8809(config-roaming-assist-policy-test)#
```

NOTE: The input parameter <HOSTNAME>, wherever used in syntaxes across this chapter, cannot include an underscore (_) character. In other words, the name of a device cannot contain an underscore.

30.1 roaming-assist-policy-instance

ROAMING ASSIST POLICY

The following table summarizes roaming assist policy configuration mode commands:

Table 30.1 *Crypto-CMP-Policy Commands*

Command	Description	Reference
action	Specifies the action to be invoked on the client	*page 30-3*
aggressiveness	Configures a roaming aggressiveness value for wireless clients	*page 30-4*
detection-threshold	Configures the detection-threshold value	*page 30-5*
disassoc-time	Configures the disassociation interval	*page 30-6*
handoff-count	Configures the handoff-count value	*page 30-7*
handoff-threshold	Configures the handoff-threshold value	*page 30-8*
monitoring-interval	Configures the client monitoring interval	*page 30-9*
sampling-interval	Configures the interval at which clients are sampled to determine their RSSI value	*page 30-10*
no	Removes or reverts this roaming assist policy settings based on the parameters passed	*page 30-11*

NOTE: For more information on common commands (clrscr, commit, help, revert, service, show, write, and exit), see *COMMON COMMANDS*.

30.1.1 action

roaming-assist-policy-instance

Specifies the action invoked on the client once it reaches a specified threshold value. The threshold values are configured based on the client load.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
action [assisted-roam|deauth|log]
```

Parameters

- `action [assisted-roam|deauth|log]`

action [assisted-roam|deauth|log]	Configures the action invoked on the client once it reaches the specified threshold value. The options are: • assisted-roam – Provides 802.11v assisted roaming facility to the client • deauth – De-authenticates the client. This is the default setting. • log – Generates a log In all three cases an event is generated. However, the message generated differs and is based on the action specified.

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#action log
rfs6000-81742D(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured action details

30.1.2 aggressiveness

roaming-assist-policy-instance

Configures a roaming aggressiveness value for wireless clients. Configuring this value increases the client's roaming capabilities in scenarios where the client's location is likely to change drastically and suddenly. For example, when a client hops on to a train that speeds up quickly. In such a scenario, the access point receives a maximum of 2 (two) messages, from the client, having relatively low RSSI value. This results in a decaying-average, which is above the specified handover-threshold value. Consequently, the client is unable to roam.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
aggressiveness [highest|lowest|medium|medium-high|medium-low]
```

Parameters

- `aggressiveness [highest|lowest|medium|medium-high|medium-low]`

aggressiveness [highest|lowest| medium| medium-high|medium-low]	Configures a roaming aggressiveness value for wireless clients. The options are: • highest – De-authenticates client in case of any degradation in the client's link quality. When selected, the access point considers only the RSSI value of the last message received from the client. • lowest – De-authenticates client only in case of significant degradation in the client's link quality. When selected, the access point uses a weighted average [80% of decaying average + 20% of last seen RSSI] as the final reported RSSI value. This is the default setting. • medium – This is an intermediate setting between not roaming and performance • medium-high – Allows roaming even if performance goes down. When selected, the access point calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the last received value. • medium-low – Allows roaming even if performance goes average. When selected, the access point calculates the client's signal strength based on average received signal as well as last received signal level, weighted towards the average value.

Example

```
nx9500-6C8809(config-roaming-assist-policy-test)#aggressiveness medium

nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 aggressiveness medium
nx9500-6C8809(config-roaming-assist-policy-test)#
```

Related Commands

no	Reverts the aggressiveness value to default (lowest)

30.1.3 detection-threshold

roaming-assist-policy-instance

Specifies the detection-threshold determining when a client is monitored

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
detection-threshold <-100--40>
```

Parameters

- `detection-threshold <-100--40>`

detection-threshold <-100--40>	Configures the detection threshold value determining when a client is monitored. The clients with bad RSSI values are monitored more frequently. • <-100--40> – Specify the RSSI value from -100 dBm - -40 dBm. The default is -75 dBm.

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#detection-threshold -90
rfs6000-81742D(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured detection threshold details

30.1.4 disassoc-time

roaming-assist-policy-instance

Configures the disassociation time. This is time period after which a disassociation message is sent.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
disassoc-time <1-10>
```

Parameters

- `disassoc-time <1-10>`

disassoc-time <1-10>	Configures the disassociation time in seconds • <1-10> – Specify a value from 1 - 10 seconds. The default is 5 seconds.

Example

```
nx9500-6C8809(config-roaming-assist-policy-test)#disassoc-time 7

nx9500-6C8809(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 disassoc-time 7
nx9500-6C8809(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured disassociation time

30.1.5 handoff-count

roaming-assist-policy-instance

Specifies the number of times a client can exceed the specified handoff-threshold value before an action is invoked

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
handoff-count <1-10>
```

Parameters

- `handoff-count <1-10>`

handoff-count <1-10>	Specifies the number of times a client can exceed the specified handoff-threshold value before an action is invoked • <1-10> – Specify a value from 1 - 10. The default is 3. If the client's RSSI increases beyond the set handoff-threshold, it is removed from the queue for monitoring and action invocation.

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#handoff-count 1
rfs6000-81742D(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured handoff-count details

30.1.6 handoff-threshold

roaming-assist-policy-instance

Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked.

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
handoff-threshold <-100--40>
```

Parameters

- `handoff-threshold <-100--40>`

handoff-threshold <-100--40>	Configures the handoff-threshold, which specifies client status for handoff-action. Once exceeded an action is invoked. • <-100--40> – Specify the RSSI value from -100 dBm - -40 dBm. The default is -80 dBm. If the client's RSSI increases beyond the set handoff-threshold, it is removed from the queue for monitoring and action invocation.

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#handoff-threshold -78
rfs6000-81742D(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured handoff-threshold details

30.1.7 monitoring-interval

roaming-assist-policy-instance

Configures the interval, in seconds, at which clients are monitored to determine if their RSSI value is below the specified handoff-threshold value

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
monitoring-interval <1-60>
```

Parameters

- `monitoring-interval <1-60>`

monitoring interval <1-60>	Specifies the interval, in seconds, at which clients are monitored to determine if their RSSI is below the specified handoff-threshold • <1-60> – Specify the duration from 1 - 60 seconds. The default is 5 seconds.

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#monitoring-interval 10
rfs6000-81742D(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured monitoring interval details

30.1.8 sampling-interval

roaming-assist-policy-instance

Configures the interval, in seconds, at which clients are sampled to determine their RSSI value

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
sampling-interval <5-60>
```

Parameters

- `sampling-interval <5-60>`

sampling-interval <5-60>	Configures the interval, in seconds, between two successive client samplings • <5-60> – Specify a value from 5 - 60 seconds. The default value is 15 seconds. Higher the RSSI value, stronger is the signal.

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#sampling-interval 20
rfs6000-81742D(config-roaming-assist-policy-test)#
```

Related Commands

no	Removes the configured sampling interval details

30.1.9 no

roaming-assist-policy-instance

Removes or reverts this roaming assist policy settings based on the parameters passed

Supported in the following platforms:

- Access Points — AP6521, AP6522, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP81XX, AP82XX, AP8432, AP8533
- Wireless Controllers — RFS4000, RFS6000
- Service Platforms — NX5500, NX7500, NX7510, NX7520, NX7530, NX9500, NX9510, NX9600, VX9000

Syntax

```
no [action|aggressiveness|detection-threshold|disassoc-time|handoff-count|
handoff-threshold|monitoring-interval|sampling-interval]
```

Parameters

- `no <PARAMETERS>`

no <PARAMETERS>	Removes or reverts this roaming assist policy settings to default based on the parameters passed

Example

```
rfs6000-81742D(config-roaming-assist-policy-test)#no action

rfs6000-81742D(config-roaming-assist-policy-test)#no detection-threshold

rfs6000-81742D(config-roaming-assist-policy-test)#no handoff-threshold

rfs6000-81742D(config-roaming-assist-policy-test)#show context
roaming-assist-policy test
 sampling-interval 20
 monitoring-interval 10
rfs6000-81742D(config-roaming-assist-policy-test)#
```

A CONTROLLER MANAGED WLAN USE CASE

This section describes the activities required to configure a WLAN. Instructions are provided using the wireless controller CLI.

- *Creating a First Controller Managed WLAN*
  - *Assumptions*
  - *Design*
  - *Using the Command Line Interface to Configure the WLAN*

A.1 Creating a First Controller Managed WLAN

CONTROLLER MANAGED WLAN USE CASE

This section describes the process of creating managed WLAN on an RFS4000 wireless controller.

Upon completion, you will have created a WLAN on a RFS4000 model wireless controller using a DHCP server to allocate IP addresses to associated wireless clients.

A.1.1 Assumptions

Verify the following conditions have been satisfied before attempting the WLAN configuration activities described in this section:

- It is assumed the RFS4000 wireless controller has the latest firmware version available.
- It is assumed the AP7161 access point also has the latest firmware version available.
- It is assumed there are no previous configurations on the wireless controller or access point and default factory configurations are running on the devices.
- It is assumed you have administrative access to the wireless controller and access point CLI.
- It is assumed the individual administrating the network is a professional network installer.

A.1.2 Design

This section defines the network design being implemented.

Figure A-1 *Network Design*

This is a simple deployment scenario, with the access points connected directly to the wireless controller. One wireless controller port is connected to an external network.

On the RFS4000 wireless controller, the GE1 interface is connected to an external network. Interfaces GE3 and GE4 are used by the access points.

On the external network, the wireless controller is assigned an IP address of 192.168.10.188. The wireless controller acts as a DHCP server for the wireless clients connecting to it, and assigns IP addresses in the range of 172.16.11.11 to 172.16.11.200. The rest of IPs in the range are reserved for devices requiring static IP addresses.

A.1.3 Using the Command Line Interface to Configure the WLAN

- *Creating a First Controller Managed WLAN*

These instructions are for configuring your first WLAN using the wireless controller CLI.

Use a serial console cable when connecting to the wireless controller for the first time. Set the following configuration when using the serial connection:

- Bits per second:*19200*
- Data Bit: *8*
- Parity: *None*
- Stop Bit: *1*
- Flow Control: *None*

The steps involved in creating a WLAN on a wireless controller are:

1 *Logging Into the Controller for the First Time*

2 *Creating a RF Domain*

3 *Creating a Wireless Controller Profile*

4 *Creating an AP Profile*

5 *Creating a DHCP Server Policy*

6 *Completing and Testing the Configuration*

A.1.3.1 Logging Into the Controller for the First Time

Using the Command Line Interface to Configure the WLAN

When powering on the wireless controller for the first time, you are prompted to replace the existing administrative password. The credentials for logging into the wireless controller for the first time are:

- User Name: *admin*
- Password: *admin123*

Ensure the new password created is strong enough to provide adequate security for the wireless controller managed network.

A.1.3.2 Creating a RF Domain

Using the Command Line Interface to Configure the WLAN

A RF Domain is a collection of configuration settings specific to devices located at the same physical deployment, such as a building or a floor. Create a RF Domain and assign the country code where the devices are deployed. This is a mandatory step, and the devices will not function as intended if this step is omitted.

The instructions in this section must be performed from the Global Configuration mode of the wireless controller. To navigate to this mode:

```
rfs4000>enable
rfs4000#
rfs4000#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
rfs4000(config)#
```

1 Create the RF Domain using the following commands:

```
rfs4000(config)#rf-domain RFDOMAIN_UseCase1
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#
```

This command creates a profile with the name *RFDOMAIN_UseCase1*.

2 Set the country code for the RF Domain.

```
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#country-code us
```

This sets the country code for this RF Domain. Save this change and exit the RF Domain profile context.

```
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#commit write
rfs4000(config-rf-domain-RFDOMAIN_UseCase1)#exit
rfs4000(config)#
```

3 To define the wireless controller's physical location, use the same RF Domain configuration.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use rf-domain RFDOMAIN_UseCase1
```

4 Commit the changes and write to the running configuration. Exit this context.

```
rfs4000(config-device-03-14-28-57-14-28)#commit write
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#
```

A.1.3.3 Creating a Wireless Controller Profile

Using the Command Line Interface to Configure the WLAN

1 The first step in creating a WLAN is to configure a profile defining the parameters applied to a wireless controller.

To create a profile:

```
rfs4000(config)#profile rfs4000 RFS4000_UseCase1
rfs4000(config-profile-RFS4000_UseCase1)#
```

This creates a profile with the name RFS4000_*UseCase1* and moves the cursor into its context. Any configuration made under this profile is available when it is applied to a device.

Configure a VLAN

2 Create the VLAN to use with the WLAN configuration. This can be done using the following commands:

```
rfs4000(config-profile-RFS4000_UseCase1)#interface vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#ip address 172.16.11.1/24
```

The above command assigns the IP address 172.16.11.1 with the mask of 255.255.255.0 to VLAN 2. Exit the VLAN 2 context.

```
rfs4000(config-profile-RFS4000_UseCase1-if-vlan2)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

3 The next step is to assign this newly created VLAN to a physical interface. In this case, VLAN 2 is mapped to GE3 and GE4 to support two access points, an AP6521 and an AP7161. The AP6521 is connected to the gigabit interface GE3 and the AP7161 to the GE4 interface.

```
rfs4000(config-profile-RFS4000_UseCase1)#interface ge 3
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#
```

4 Map VLAN 2 to this interface. This assigns the IP address to the selected physical interface.

```
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge3)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

5 Similarly, map the defined VLAN 2 to the GE4 interface.

```
rfs4000(config-profile-1_UseCase1)#interface ge 4
rfs4000(config-profile-RFS4000_UseCase1-if-ge4)#switchport access vlan 2
rfs4000(config-profile-RFS4000_UseCase1-if-ge4)#exit
rfs4000(config-profile-RFS4000_UseCase1)#
```

6 Exit the profile and save it.

```
rfs4000(config-profile-RFS4000_UseCase1)#exit
rfs4000(config)#commit write
```

Configure the Wireless Controller to use the Profile

7 Before the wireless controller can be further configured, the profile must be applied to the wireless controller.

```
rfs4000(config)#self
rfs4000(config-device-03-14-28-57-14-28)#
rfs4000(config-device-03-14-28-57-14-28)#use profile RFS4000_UseCase1
rfs4000(config-device-03-14-28-57-14-28)#exit
rfs4000(config)#commit write
```

Create a WLAN

8 Use the following commands to create a WLAN:

```
rfs4000(config)#wlan 1
rfs4000(config-wlan-1)#
```

9 Configure the SSID for the WLAN. This is the value that identifies and helps differentiate this WLAN.

```
rfs4000(config-wlan-1)#ssid WLAN_USECASE_01
```

10 Enable the SSID to be broadcast so wireless clients can find it and associate.

```
rfs4000(config-wlan-1)#broadcast-ssid
```

11 Associate VLAN 2 to the WLAN and exit.

```
rfs4000(config-wlan-1)#vlan 2
rfs4000(config-wlan-1)#exit
```

12 Commit the Changes

Once these changes have been made, they have to be committed before proceeding.

```
rfs4000(config)#commit write
```

A.1.3.4 Creating an AP Profile

Using the Command Line Interface to Configure the WLAN

An AP profile provides a method of applying common settings to access points of the same model. The profile significantly reduces the time required to configure access points within a large deployment. For more information, see:

- *Creating an AP6521 Profile*
- *Creating an AP7161 Profile*

A.1.3.4.1 Creating an AP6521 Profile

Creating an AP Profile

An AP6521's firmware is updated directly by its associated wireless controller. The process is automatic, and no intervention is required. To create a profile for use with an AP6521:

```
rfs4000(config)#profile ap6521 AP6521_UseCase1
rfs4000(config-profile-AP6521_UseCase1)#
```

1 Assign the access point to be a member of the same VLAN defined in *Creating an AP Profile on page A-5*. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of VLAN 2.

```
rfs4000(config-profile-AP6521_UseCase1)#interface vlan 2
rfs4000(config-profile-AP6521_UseCase1-if-vlan2)#
```

2 Configure this VLAN to use DHCP, so any device that is associated using this access point is automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-AP6521_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-AP6521_UseCase1-if-vlan2)#exit
```

3 The VLAN has to be mapped to a physical interface on the access point. Since the only available physical interface on the AP6521 is GE1, this VLAN is mapped to it.

```
rfs4000(config-profile-AP6521_UseCase1)#interface ge 1
rfs4000(config-profile-AP6521_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-AP6521_UseCase1-if-ge1)#exit
```

4 Before a WLAN can be implemented, it has to be mapped to a radio on the access point. An AP6521 has 2 radios, in this scenario, both radios are utilized.

```
rfs4000(config-profile-AP6521_UseCase1)#interface radio 1
rfs4000(config-profile-AP6521_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-AP6521_UseCase1-if-radio1)#exit
rfs4000(config-profile-AP6521_UseCase1)#interface radio 2
rfs4000(config-profile-AP6521_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-AP6521_UseCase1-if-radio2)#exit
rfs4000(config-profile-AP6521_UseCase1)#
```

5 Commit the changes made to this profile and exit.

```
rfs4000(config-profile-AP6521_UseCase1)#commit write
rfs4000(config-profile-AP6521_UseCase1)#exit
rfs4000(config)#
```

6 Apply this Profile to the discovered AP6521.

7 Access the discovered access point using the following command. The discovered device's MAC address is used to access its context.

```
rfs4000(config)#ap6521 00-A0-F8-00-00-01
rfs4000(config-device-00-A0-F8-00-00-01)#
```

8 Assign the AP profile to this AP6521 access point.

```
rfs4000(config-device-00-A0-F8-00-00-01)#use profile AP6521_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
```

9 Apply the RF Domain profile to the AP.

10 Apply the previously created RF Domain to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the country code of its associated wireless controller.

```
rfs4000(config-device-00-A0-F8-00-00-01)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-A0-F8-00-00-01)#commit write
rfs4000(config-device-00-A0-F8-00-00-01)#exit
rfs4000(config)#
```

A.1.3.4.2 Creating an AP7161 Profile

Creating an AP Profile

To create a profile for use with an AP7161:

```
rfs4000(config)#profile ap7161 AP7161_UseCase1
rfs4000(config-profile-AP7161_UseCase1)#
```

1 Set the access point to be a member of the same VLAN defined in *Creating an AP Profile on page A-5*. In this section, the VLAN was defined as VLAN 2. Configure the access point to be a member of the VLAN 2.

```
rfs4000(config-profile-AP7161_UseCase1)#interface vlan 2
rfs4000(config-profile-AP7161_UseCase1-if-vlan2)#
```

2 Configure this VLAN to use DHCP, so any device associated using this access point is automatically assigned a unique IP address. Once completed, exit this context.

```
rfs4000(config-profile-AP7161_UseCase1-if-vlan2)#ip address dhcp
rfs4000(config-profile-AP7161_UseCase1-if-vlan2)#exit
```

3 The configured VLAN has to be mapped to a physical interface on the access point. Map VLAN 2 to the GE1 and GE2 interfaces on the AP7161. To configure the GE1 interface:

```
rfs4000(config-profile-AP7161_UseCase1)#interface ge 1
rfs4000(config-profile-AP7161_UseCase1-if-ge1)#switchport access vlan 2
rfs4000(config-profile-AP7161_UseCase1-if-ge1)#exit
```

4 Similarly configure the GE2 interface.

```
rfs4000(config-profile-AP7161_UseCase1)#interface ge 2
rfs4000(config-profile-AP7161_UseCase1-if-ge2)#switchport access vlan 2
rfs4000(config-profile-AP7161_UseCase1-if-ge2)#exit
```

5 Before the WLAN can be implemented, it has to be mapped to the physical radio on the access point. An AP7161 has 3 radios (on certain models), two of which can be configured for WLAN support. In this scenario, two radios are used.

```
rfs4000(config-profile-AP7161_UseCase1)#interface radio 1
rfs4000(config-profile-AP7161_UseCase1-if-radio1)#wlan 1
rfs4000(config-profile-AP7161_UseCase1-if-radio1)#exit
rfs4000(config-profile-AP7161_UseCase1)#interface radio 2
rfs4000(config-profile-AP7161_UseCase1-if-radio2)#wlan 1
rfs4000(config-profile-AP7161_UseCase1-if-radio2)#exit
rfs4000(config-profile-AP7161_UseCase1)#
```

6 Commit the changes made to the profile and exit this context.

```
rfs4000(config-profile-AP7161_UseCase1)#commit write
rfs4000(config-profile-AP7161_UseCase1)#exit
rfs4000(config)#
```

7 Apply this Profile to the Discovered AP7161.

8 Access the discovered access point using the following command. The discovered device's MAC address is used to access its context.

```
rfs4000(config)#ap7161 00-23-68-16-C6-C4
rfs4000(config-device-00-23-68-16-C6-C4)#
```

9 Assign the AP profile to this access point.

```
rfs4000(config-device-00-23-68-16-C6-C4)#use profile AP7161_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
```

10 Apply the RF Domain profile to the AP.

11 Apply the previously created RF Domain to enable a country code to be assigned to the discovered access point. A discovered access point only works properly if its country code is the same as its associated wireless controller.

```
rfs4000(config-device-00-23-68-16-C6-C4)#use rf-domain RFDOMAIN_UseCase1
rfs4000(config-device-00-23-68-16-C6-C4)#commit write
rfs4000(config-device-00-23-68-16-C6-C4)#Exit
rfs4000(config)#
```

A.1.3.5 Creating a DHCP Server Policy

Using the Command Line Interface to Configure the WLAN

The DHCP server policy defines the parameters required to run a DHCP server on the wireless controller and assign IP addresses automatically to devices that associate. Configuring DHCP enables the reuse of a limited set of IP addresses.

To create a DHCP server policy:

```
rfs4000-37FABE(config)#dhcp-server-policy DHCP_POLICY_UseCase1
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#
```

The following table displays how IP addresses are used.

Table A.1 *IP Address Usage*

IP Range	Usage
172.16.11.1 till 172.16.11.10	Reserved for devices that require a static IP address
172.16.11.11 till 172.16.11.200	Range of IP addresses that can be assigned using the DHCP server.
172.16.11.201 till 172.16.11.254	Reserved for devices that require a static IP address

In the table, the IP address range of 172.16.11.11 to 172.16.11.200 is available using the DHCP server. To configure the DHCP server:

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#dhcp-pool
DHCP_POOL_USECASE1_01
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#
```

1 Configure the address range as follows:

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#address range 172.16.11.11 172.16.11.200
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#
```

2 Configure the IP pool used with a network segment. This starts the DHCP server on the specified interface.

```
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#network 172.16.11.0/24
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1-pool-
DHCP_POOL_USECASE1_01)#exit
rfs4000-37FABE(config-dhcp-policy-DHCP_POLICY_UseCase1)#exit
rfs4000-37FABE(config)#commit write
```

Configure the RFS4000 to use the DHCP Policy

3 For the DHCP to work properly, the new DHCP Server Policy must be applied to the wireless controller. To apply the DHCP Server Policy to the wireless controller:

```
rfs4000-37FABE(config)#self
rfs4000-37FABE(config-device-03-14-28-57-14-28)#use dhcp-server-policy
DHCP_POLICY_UseCase1
rfs4000-37FABE(config-device-03-14-28-57-14-28)#commit write
rfs4000-37FABE(config-device-03-14-28-57-14-28)#exit
rfs4000-37FABE(config)#
```

A.1.3.6 Completing and Testing the Configuration

Using the Command Line Interface to Configure the WLAN

A wireless client must be configured to associate with the wireless controller managed WLAN. The following information must be defined:

- SSID: `WLAN_USECASE_01`
- Country: Same as the country configured in *Creating a RF Domain on page A-3*. In this scenario, the country code is set to US.
- Mode: Infrastructure

With the WLAN set to beacon, use the wireless client's discovery client to discover the configured WLAN and associate.

B PUBLICLY AVAILABLE SOFTWARE

B.1 General Information

This document contains information regarding licenses, acknowledgments and required copyright notices for open source packages used in the following products:

Access Points

- AP6521, AP6522, AP6522M, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8122, AP8132, AP8163, AP8232, AP8432 and AP8533.

Wireless Controllers and Service Platforms

- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX5500, NX5500E, NX7500, NX75XX, NX7510E, NX9500, NX9510, NX9600, NX9610, VX9000, VX9000E

B.2 Open Source Software Used

The Support site, located at www.extremenetworks.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Name	Version	URL	License
Apache Web Server	1.3.41	*http://www.apache.org/*	*Apache License, Version 2.0*
Asterisk	1.2.24	*http://www.asterisk.org/*	*GNU General Public License 2.0*
accepts	1.2.10	*http://registry.npmjs.org/accepts/-/accepts-1.2.10.tgz*	*MIT License*
advas	0.2.3	*http://advas.sourceforge.net/*	*GNU General Public License, version 2*
alivepdf	0.1.4.9	*https://code.google.com/p/alivepdf/*	*MIT License*
apscheduler	3.0.1	*https://pypi.python.org/pypi/APScheduler/*	*MIT License*
async	1.3.0	*http://registry.npmjs.org/async/-/async-1.3.0.tgz*	*MIT License*
autoconf	2.69	*http://www.gnu.org/software/autoconf/*	*GNU General Public License, version 2*
automake	1.11.6	*http://www.gnu.org/software/automake/*	*GNU General Public License, version 2*
bash	4.2	*http://www.gnu.org/software/bash/*	*GNU General Public License, version 2*
binutils	2.23	*http://www.gnu.org/software/binutils/*	*GNU General Public License, version 2*
bison	2.3	*http://www.gnu.org/software/bison/*	*GNU General Public License, version 2*
bluez	5.7	*http://www.bluez.org/*	*GNU General Public License, version 2*
body-parser	1.13.2	*http://registry.npmjs.org/body-parser/-/body-parser-1.13.2.tgz*	*MIT License*
bridge	1.0.4	*http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/*	*GNU General Public License, version 2*
bridge-utils	1.0.4	*http://sourceforge.net/projects/bridge/*	*GNU General Public License, version 2*
buffer-crc32	0.2.5	*http://registry.npmjs.org/buffer-crc32/-/buffer-crc32-0.2.5.tgz*	*MIT License*
busybox	1.14.4	*http://www.busybox.net/*	*GNU General Public License, version 2*

Name	Version	URL	License
bytes	2.1.0	*http://registry.npmjs.org/bytes/-/bytes-2.1.0.tgz*	*MIT License*
colors	1.1.2	*http://registry.npmjs.org/colors/-/colors-1.1.2.tgz*	*MIT License*
compression	1.5.1	*http://registry.npmjs.org/compression/-/compression-1.5.1.tgz*	*MIT License*
conect-mongo	0.8.2	*http://registry.npmjs.org/connect-mongo/-/connect-mongo-0.8.2.tgz*	*MIT License*
cookie	0.1.3	*http://registry.npmjs.org/cookie/-/cookie-0.1.3.tgz*	*MIT License*
cookie-parser	1.3.5	*http://registry.npmjs.org/cookie-parser/-/cookie-parser-1.3.5.tgz*	*MIT License*
cookie-signature	1.0.6	*http://registry.npmjs.org/cookie-signature/-/cookie-signature-1.0.6.tgz*	*MIT License*
cuint	0.2.0	*http://registry.npmjs.org/cuint/-/cuint-0.2.0.tgz*	*MIT License*
cycle	1.0.3	*https://registry.npmjs.org/cycle/-/cycle-1.0.3.tgz*	*MIT License*
czjson	1.0.8	*https://pypi.python.org/pypi/czjson/1.0.8*	*GNU Lesser General Public License 2.1*
dash	0.5.7	*http://gondor.apana.org.au/~herbert/dash/*	*The BSD License*
debug	2.2.0	*https://registry.npmjs.org/debug/-/debug-2.2.0.tgz*	*MIT License*
depd	1.0.1	*http://registry.npmjs.org/depd/-/depd-1.0.1.tgz*	*MIT License*
dfu-util	0.8	*http://dfu-util.gnumonks.org/*	*GNU General Public License, version 2*
dhcp	3.0.3	*http://www.isc.org/software/dhcp*	*ISC License*
diffutils	2.8.1	*http://www.gnu.org/software/diffutils/*	*GNU General Public License, version 2*
dmalloc	5.5.2	*http://dmalloc.com/*	None
dmidecode	2.11	*http://savannah.nongnu.org/projects/dmidecode/*	*GNU General Public License, version 2*
dnsmasq	2.47	*http://www.thekelleys.org.uk/dnsmasq/doc.html*	*GNU General Public License, version 2*
dosfstools	2.11	*http://www.daniel-baumann.ch/software/dosfstools/*	*GNU General Public License, version 2*
dropbear	0.55	*http://matt.ucc.asn.au/dropbear/dropbear.html*	*DropBear License*
e2fsprogs	1.41.13	*http://e2fsprogs.sourceforge.net/*	*GNU General Public License, version 2*

Name	Version	URL	License
ejs	2.3.3	*http://registry.npmjs.org/ejs/-/ejs-2.3.3.tgz*	*Apache License, Version 2.0*
engine.io	1.5.2	*http://registry.npmjs.org/engine.io/-/engine.io-1.5.2.tgz*	*MIT License*
escape-html	1.0.2	*http://registry.npmjs.org/escape-html/-/escape-html-1.0.2.tgz*	*MIT License*
ethtool	2.6.35	*http://www.kernel.org/pub/software/network/ethtool/*	*GNU General Public License, version 2*
event-loop-lag	1.1.0	*http://registry.npmjs.org/event-loop-lag/-/event-loop-lag-1.1.0.tgz*	*MIT License*
express	4.13.1	*http://registry.npmjs.org/express/-/express-4.13.1.tgz*	*MIT License*
express-session	1.11.3	*http://registry.npmjs.org/express-session/-/express-session-1.11.3.tgz*	*MIT License*
eyes	0.1.8	*http://github.com/cloudhead/eyes.js*	*MIT License*
finalhandler	0.4.0	*http://registry.npmjs.org/finalhandler/-/finalhandler-0.4.0.tgz*	*MIT License*
flashrom	0.9.4	*http://flashrom.org/Flashrom*	*GNU General Public License, version 2*
flex	4.5.1.21328	*http://flex.sourceforge.net/*	*The BSD License*
fluks	0.2	*https://github.com/markuspeloquin/fluks*	*MIT License*
freedos	4.5.1.21328	*http://www.freedos.org/download/*	*GNU General Public License, version 2*
freeipmi	1.1	*http://www.gnu.org/software/freeipmi/*	*GNU General Public License, version 3*
fresh	0.3.0	*http://registry.npmjs.org/fresh/-/fresh-0.3.0.tgz*	*MIT License*
futures	2.2.0	*https://github.com/agronholm/pythonfutures*	*The BSD License*
gcc	4.1.2	*http://gcc.gnu.org/*	*GNU General Public License, version 2*
gdb	7.2	*http://www.gnu.org/software/gdb/*	*GNU General Public License, version 3*
gdbm	1.8.3	*http://www.gnu.org/s/gdbm/*	*GNU General Public License, version 2*
genext2fs	1.4.1	*http://genext2fs.sourceforge.net/*	*GNU General Public License, version 2*
glib2	2.30.2	*http://www.gtk.org/*	*GNU Lesser General Public License 2.1*
glibc	2.7	*http://www.gnu.org/software/libc/*	*GNU General Public License, version 2*

Name	Version	URL	License
has-binary-data	0.1.5	*http://registry.npmjs.org/has-binary-data/-/has-binary-data-0.1.5.tgz*	*MIT License*
hdparm	9.38	*http://sourceforge.net/projects/hdparm/*	*GNU General Public License, version 2*
hooks	0.3.2	*http://registry.npmjs.org/hooks/-/hooks-0.3.2.tgz*	*MIT License*
hostapd	0.6.9	*http://hostap.epitest.fi/hostapd/*	*GNU General Public License, version 2*
hotplug	1.3	*http://sourceforge.net/projects/linux-hotplug/*	*GNU General Public License, version 2*
hotplug2	0.9	*http://isteve.bofh.cz/~isteve/hotplug2/*	*GNU General Public License, version 2*
i2ctools	3.0.3	*http://www.lm-sensors.org/wiki/I2CTools*	*GNU General Public License, version 2*
iconv-lite	0.4.11	*http://registry.npmjs.org/iconv-lite/-/iconv-lite-0.4.11.tgz*	*MIT License*
igb	5.2.9.4	*http://sourceforge.net/projects/e1000/*	*GNU General Public License, version 2*
ipaddr	2.1.0	*http://code.google.com/p/ipaddr-py/*	*Apache License, Version 2.0*
ipkg-utils	1.7	*http://www.handhelds.org/sources.html*	*GNU General Public License, version 2*
ipmitool	1.8.11	*http://ipmitool.sourceforge.net/*	*The BSD License*
iproute2	050816	*http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2*	*GNU General Public License, version 2*
iptables	1.4.3	*http://www.netfilter.org/projects/iptables/index.html*	*GNU General Public License, version 2*
ipxe	1.0.0	*http://ipxe.org/*	*GNU General Public License, version 2*
isstream	0.1.2	*https://registry.npmjs.org/isstream/-/isstream-0.1.2.tgz*	*MIT License*
js-yaml	3.3.1	*http://registry.npmjs.org/js-yaml/-/js-yaml-3.3.1.tgz*	*MIT License*
kerberos	None	*http://web.mit.edu/Kerberos/*	*GNU General Public License, version 2*
kexec-tools	2.0.3	*http://kernel.org/pub/linux/utils/kernel/kexec/*	*GNU General Public License, version 2*
libbson	1.1.0	*http://github.com/mongodb/libbson*	*Apache License, Version 2.0*
libcares	1.7.1	*http://c-ares.haxx.se/*	*The BSD License*

Name	Version	URL	License
libcurl	7.30.0	*http://curl.haxx.se/libcurl/*	*The BSD License*
libdevmapper	2.02.66	*ftp://sources.redhat.com/pub/lvm2/old*	*GNU Lesser General Public License 2.1*
libexpat	2.0.0	*http://expat.sourceforge.net/*	*MIT License*
libffi	3.0.7	*http://sourceware.org/libffi/*	*MIT License*
libgcrypt	1.4.5	*ftp://ftp.gnupg.org/GnuPG/libgcrypt/*	*GNU Lesser General Public License 2.1*
libgmp	4.2.2	*http://gmplib.org/*	*GNU Lesser General Public License, version 3.0*
libgnutls	3.2.12	*ftp://ftp.gnupg.org/GnuPG/gnutls/v3.0/*	*GNU Lesser General Public License, version 3.0*
libgpg-error	1.6	*ftp://ftp.gnupg.org/GnuPG/libgpg-error/*	*GNU Lesser General Public License 2.1*
libharu	2.1.0	*http://libharu.org/*	*MIT License*
libhttp-parser	None	*None*	*MIT License*
libiconv	1.14	*http://savannah.gnu.org/projects/libiconv/*	*GNU General Public License 2.0*
libjson	0.10	*http://sourceforge.net/projects/libjson/*	*The BSD License*
libkerberos	0.1	*http://web.mit.edu/kerberos/dist/*	*The BSD License*
libncurses	5.4	*http://www.gnu.org/software/ncurses/*	*MIT License*
libnettle	2.7	*http://www.lysator.liu.se/~nisse/nettle/*	*GNU Lesser General Public License 2.1*
libnuma	2.0.10	*https://github.com/numactl/numactl/*	*GNU Lesser General Public License, version 2.0*
libpam	1.1.1	*http://www.kernel.org/pub/linux/libs/pam/*	*The BSD License*
libpcap	1.0.0	*http://www.tcpdump.org/*	*The BSD License*
libpcre	8.21	*ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/*	*The BSD License*
libpopt	1.14	*http://freecode.com/projects/popt*	*MIT License*
libraryopt	1.01	*http://sourceforge.net/projects/libraryopt/*	*GNU General Public License, version 2*
libreadline	4.3	*http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html*	*GNU General Public License, version 2*
libtool	2.4.2	*http://www.gnu.org/software/libtool/*	*GNU General Public License, version 2*

Name	Version	URL	License
libusb	0.1.12	*http://www.libusb.org/*	*GNU Lesser General Public License, version 2.0*
libusb	1.0.18	*http://www.libusb.org/*	*GNU Lesser General Public License, version 2.0*
libvirt	0.9.11	*http://libvirt.org/sources/*	*GNU Lesser General Public License 2.1*
libxml2	2.8.0	*http://xmlsoft.org/*	*MIT License*
libxslt	1.1.26	*http://xmlsoft.org/xslt/*	*MIT License*
lighttpd	1.4.37	*http://www.lighttpd.net/*	*MIT License*
lilo	22.6	*http://lilo.alioth.debian.org/*	*The BSD License*
linux	2.6.28.9	*http://www.kernel.org/*	*GNU General Public License, version 2*
linux	2.6.35.9	*http://www.kernel.org/*	*GNU General Public License, version 2*
lodash	3.10.0	*http://registry.npmjs.org/lodash/-/lodash-3.10.0.tgz*	*MIT License*
log-timestamp	0.1.2	*http://registry.npmjs.org/log-timestamp/-/log-timestamp-0.1.2.tgz*	*MIT License*
ltp	20130904	*https://github.com/linux-test-project/ltp*	*GNU General Public License, version 2*
lxml	2.3beta1	*http://lxml.de/*	*The BSD License*
lzma	4.32	*http://www.7-zip.org/sdk.html*	*GNU Lesser General Public License, version 2.0*
lzma	4.57	*http://www.7-zip.org/sdk.html*	*GNU Lesser General Public License, version 2.0*
lzo	2.03	*http://www.oberhumer.com/opensource/lzo/*	*GNU General Public License, version 2*
M2Crypto	0.21.1	*http://chandlerproject.org/bin/view/Projects/MeTooCrypto*	*The BSD License*
m4	1.4.16	*http://www.gnu.org/software/m4/*	*GNU General Public License, version 2*
madwifi	trunk-r3314	*http://madwifi-project.org/*	*The BSD License*
mdadm	3.2.2	*http://neil.brown.name/blog/mdadm*	*GNU General Public License, version 2*
media-typer	0.3.0	*http://registry.npmjs.org/media-typer/-/media-typer-0.3.0.tgz*	*MIT License*
memtester	4.0.8	*http://pyropus.ca/software/memtester/*	*GNU General Public License, version 2*

Name	Version	URL	License
merge-descriptors	1.0.0	*http://registry.npmjs.org/merge-descriptors/-/merge-descriptors-1.0.0.tgz*	*MIT License*
method-override	2.3.4	*http://registry.npmjs.org/method-override/-/method-override-2.3.4.tgz*	*MIT License*
methods	1.1.1	*http://registry.npmjs.org/methods/-/methods-1.1.1.tgz*	*MIT License*
mii-diag	2.09	*http://freecode.com/projects/mii-diag*	*GNU General Public License, version 2*
mkyaffs	None	*http://www.yaffs.net/*	*GNU General Public License, version 2*
mod_ssl	2.8.3.1-1.3.41	*http://www.modssl.org/*	*The BSD License*
mongo-c-driver	1.1.0	*http://github.com/mongodb/mongo-c-driver*	*Apache License, Version 2.0*
mongo-python-driver	2.7.1	*http://github.com/mongodb/mongo-python-driver*	*Apache License, Version 2.0*
mongodb	3.0.5	*http://www.mongodb.org/*	*GNU Lesser General Public License, version 3.0*
mongoose	4.0.7	*http://registry.npmjs.org/mongoose/-/mongoose-4.0.7.tgz*	*MIT License*
mpath	0.2.1	*http://registry.npmjs.org/mpath/-/mpath-0.2.1.tgz*	*MIT License*
mpromise	0.5.5	*http://registry.npmjs.org/mpromise/-/mpromise-0.5.5.tgz*	*MIT License*
mquery	1.6.2	*http://registry.npmjs.org/mquery/-/mquery-1.6.2.tgz*	*MIT License*
ms	0.7.1	*http://registry.npmjs.org/ms/-/ms-0.7.1.tgz*	*MIT License*
mtd	2009-05-05	*http://www.linux-mtd.infradead.org/*	*GNU General Public License, version 2*
mtd-utils	1.4.4	*http://www.linux-mtd.infradead.org/*	*GNU General Public License, version 2*
mtd-utils	2009-05-05	*http://www.linux-mtd.infradead.org/*	*GNU General Public License, version 2*
muri	1.1.0	*http://registry.npmjs.org/muri/-/muri-1.1.0.tgz*	*MIT License*
nano	1.2.4	*http://www.nano-editor.org/*	*GNU General Public License, version 2*
net-snmp	5.3.0.1	*http://net-snmp.sourceforge.net/*	*The BSD License*
no-vnc	None	*http://kanaka.github.io/noVNC/*	*Mozilla Public License, version 2*

Name	Version	URL	License
node-mongodb-native	1.4.35	*http://github.com/mongodb/node-mongodb-native*	*Apache License, Version 2.0*
node.js	0.12.7	*http://nodejs.org/*	*MIT License*
ntp	4.2.6p4	*http://www.ntp.org/index.html*	*The BSD License*
numactl	2.0.10	*https://github.com/numactl/numactl/*	*GNU General Public License, version 2*
Open Scales	2.2	*http://openscales.org/*	*GNU Lesser General Public License, version 3.0*
OpenStreetMap		*http://www.openstreetmap.org/*	*Creative Commons Attribution-ShareAlike License, version 3.0*
on-headers	1.0.0	*http://registry.npmjs.org/on-headers/-/on-headers-1.0.0.tgz*	*MIT License*
openldap	2.4.40	*http://www.openldap.org/foundation/*	*The Open LDAP Public License*
openllpd	0.0.3alpha	*http://openlldp.sourceforge.net/*	*GNU General Public License, version 2*
openssh	6.6p1	*http://www.openssh.com/*	*The BSD License*
openssl	0.9.8zg	*http://www.openssl.org/*	*OpenSSL License*
openssl	1.0.0i	*http://www.openssl.org/*	*OpenSSL License*
openssl	1.0.1g	*http://www.openssl.org/*	*OpenSSL License*
openssl-fips	1.2.3	*http://www.openssl.org/*	*OpenSSL License*
openwrt	trunk-r15025	*http://www.openwrt.org/*	*GNU General Public License, version 2*
opkg	trunk-r4564	*http://code.google.com/p/opkg/*	*GNU General Public License, version 2*
oprofile	0.9.2	*http://oprofile.sourceforge.net/news/*	*GNU Lesser General Public License 2.1*
ProGuard	4.8	*http://proguard.sourceforge.net/*	*GNU General Public License, version 2*
PyPDF2	1.23	*http://mstamy2.github.com/PyPDF2*	*The BSD License*
parseurl	1.3.0	*http://registry.npmjs.org/parseurl/-/parseurl-1.3.0.tgz*	*MIT License*
path-to-regexp	1.2.0	*http://registry.npmjs.org/path-to-regexp/-/path-to-regexp-1.2.0.tgz*	*MIT License*
pciutils	3.1.8	*http://mj.ucw.cz/sw/pciutils/*	*GNU General Public License, version 2*

Name	Version	URL	License
pdnsd	1.2.5	*http://members.home.nl/p.a.rombouts/pdnsd/*	*GNU General Public License, version 2*
picocom	1.6	*http://code.google.com/p/picocom/*	*GNU General Public License, version 2*
pillow	2.8.1	*http://python-pillow.github.io/*	*MIT License*
ping	1.0	*None*	*The BSD License*
pkg-config	0.22	*http://pkg-config.freedesktop.org/wiki/*	*GNU General Public License, version 2*
portmap	6.0	*http://neil.brown.name/portmap/*	*The BSD License*
posix	2.0.1	*http://registry.npmjs.org/posix/-/posix-2.0.1.tgz*	*MIT License*
ppp	2.4.5	*http://ppp.samba.org/ppp/*	*The BSD License*
ppp	2.4.3	*http://ppp.samba.org/ppp/*	*The BSD License*
preppy	2.3.1	*https://bitbucket.org/rptlab/preppy*	*The BSD License*
procname	0.2	*http://code.google.com/p/procname/*	*GNU Lesser General Public License, version 2.0*
procps	3.2.8	*http://procps.sourceforge.net/*	*GNU General Public License, version 2*
proxy-addr	1.0.8	*http://registry.npmjs.org/proxy-addr/-/proxy-addr-1.0.8.tgz*	*MIT License*
psmisc	22.8	*http://sourceforge.net/projects/psmisc/*	*GNU General Public License, version 2*
pure-ftpd	1.0.22	*http://www.pureftpd.org/project/pure-ftpd*	*The BSD License*
pychecker	0.8.18	*http://pychecker.sourceforge.net/*	*The BSD License*
pyparsing	1.5.1	*http://sourceforge.net/projects/pyparsing/*	*The BSD License*
pytz	2014.10	*http://pythonhosted.org/pytz*	*MIT License*
pyxapi	0.1	*http://www.pps.jussieu.fr/%7Eylg/PyXAPI/*	*GNU General Public License, version 2*
pyyaml	3.11	*http://pyyaml.org/*	*MIT License*
qdbm	1.8.77	*http://qdbm.sourceforge.net/*	*GNU General Public License, version 2*
qs	4.0.0	*http://registry.npmjs.org/qs/-/qs-4.0.0.tgz*	*The BSD License*
quagga	0.99.16	*http://www.quagga.net*	*GNU General Public License, version 2*
quilt	0.47	*http://savannah.nongnu.org/projects/quilt/*	*GNU General Public License, version 2*

Name	Version	URL	License
radius	2.2.3	*http://freeradius.org/*	*GNU General Public License, version 2*
range-parser	1.0.2	*http://registry.npmjs.org/range-parser/-/range-parser-1.0.2.tgz*	*MIT License*
raw-body	2.1.2	*http://registry.npmjs.org/raw-body/-/raw-body-2.1.2.tgz*	*MIT License*
redis	3.0.3	*http://redis.io/*	*The BSD License*
redis	0.12.1	*http://registry.npmjs.org/redis/-/redis-0.12.1.tgz*	*MIT License*
regexp-clone	0.0.1	*http://registry.npmjs.org/regexp-clone/-/regexp-clone-0.0.1.tgz*	*MIT License*
report-lab	3.1.44	*http://www.reportlab.com*	*The BSD License*
rp-pppoe	3.1.0	*http://www.roaringpenguin.com/products/pppoe*	*GNU General Public License, version 2*
rsync	3.0.6	*http://rsync.samba.org/*	*GNU General Public License, version 3*
safestr	1.0.3	*http://www.zork.org/*	*The BSD License*
samba	3.5.1	*http://www.samba.org*	*GNU General Public License, version 3*
sed	4.1.2	*http://www.gnu.org/software/sed/*	*GNU General Public License, version 2*
semaphore	1.0.3	*http://registry.npmjs.org/semaphore/-/semaphore-1.0.3.tgz*	*MIT License*
send	0.13.0	*http://registry.npmjs.org/send/-/send-0.13.0.tgz*	*MIT License*
serve-static	1.10.0	*http://registry.npmjs.org/serve-static/-/serve-static-1.10.0.tgz*	*MIT License*
setproctitle	1.1.8	*http://code.google.com/p/py-setproctitle*	*The BSD License*
setuptools	11.3.1	*https://bitbucket.org/pypa/setuptools*	*Python License, Version 2 (Python-2.0)*
sliced	1.0.1	*http://registry.npmjs.org/sliced/-/sliced-1.0.1.tgz*	*MIT License*
smarttools	6.2	*http://smartmontools.sourceforge.net*	*GNU General Public License, version 2*
snmpagent	5.0.9	*http://sourceforge.net/*	*The BSD License*
socket.io	1.3.6	*http://registry.npmjs.org/socket.io/-/socket.io-1.3.6.tgz*	*MIT License*
socket.io-adapter	0.3.1	*http://registry.npmjs.org/socket.io-adapter/-/socket.io-adapter-0.3.1.tgz*	*MIT License*

Name	Version	URL	License
socket.io-adapter-mongo	0.1.4	*http://registry.npmjs.org/socket.io-adapter-mongo/-/socket.io-adapter-mongo-0.1.4.tgz*	*MIT License*
socket.io-client	1.3.6	*http://registry.npmjs.org/socket.io-client/-/socket.io-client-1.3.6.tgz*	*MIT License*
socket.io-parser	2.2.4	*http://registry.npmjs.org/socket.io-parser/-/socket.io-parser-2.2.4.tgz*	*MIT License*
sqlite3	3070900	*http://www.sqlite.org/*	None
squashfs	3.0	*http://squashfs.sourceforge.net/*	*GNU General Public License, version 2*
squid	2.7.STABLE9	*http://www.squid-cache.org/*	*GNU General Public License, version 2*
stack-trace	0.0.9	*https://registry.npmjs.org/stack-trace/-/stack-trace-0.0.9.tgz*	*MIT License*
stackless python	2.7.5	*http://www.stackless.com/*	*GNU General Public License, version 2*
sticky-session	0.1.0	*http://registry.npmjs.org/sticky-session/-/sticky-session-0.1.0.tgz*	*MIT License*
strace	4.5.20	*http://sourceforge.net/projects/strace/*	*The BSD License*
stress	1.0.4	*http://people.seas.harvard.edu/~apw/stress/*	*GNU General Public License, version 2*
strongswan	4.4.0	*http://www.strongswan.org*	*GNU General Public License, version 2*
stunnel	4.31	*http://www.stunnel.org/*	*GNU General Public License, version 2*
svg2rlg	0.3	*http://code.google.com/p/svg2rlg/*	*The BSD License*
sysstat	9.0.5	*http://sebastien.godard.pagesperso-orange.fr/*	*GNU General Public License, version 2*
tar	1.17	*http://www.gnu.org/software/tar/*	*GNU General Public License, version 2*
tcpdump	4.0.0	*http://www.tcpdump.org/*	*The BSD License*
tinyproxy	1.8.3	*https://banu.com/tinyproxy/*	*GNU General Public License, version 2*
type-is	1.6.4	*http://registry.npmjs.org/type-is/-/type-is-1.6.4.tgz*	*MIT License*
tz	2014b	*http://www.iana.org/time-zones/repository/releases/*	*GNU General Public License, version 2*
u-boot	trunk-2010-03-30	*http://www.denx.de/wiki/U-Boot/*	*GNU General Public License, version 2*

Name	Version	URL	License
u-boot	trunk-2010-05-10	*http://www.denx.de/wiki/U-Boot/*	*GNU General Public License, version 2*
uClibc	0.9.29	*http://www.uclibc.org/*	*GNU General Public License, version 2*
uClibc	0.9.30.2	*http://www.uclibc.org/*	*GNU General Public License, version 2*
uci	0.7.5	*http://www.openwrt.org/*	*GNU General Public License, version 2*
udev	147	*https://launchpad.net/udev*	*GNU General Public License, version 2*
udev	r147	*http://www.kernel.org/pub/linux/utils/kernel/hotplug/*	*GNU General Public License, version 2*
usbutils	0.73	*http://www.linux-usb.org/*	*GNU General Public License, version 2*
util-linux	2.20	*http://www.kernel.org/pub/linux/utils/util-linux/*	*GNU General Public License, version 2*
utils-merge	1.0.0	*http://registry.npmjs.org/utils-merge/-/utils-merge-1.0.0.tgz*	*MIT License*
valgrind	3.5.0	*http://valgrind.org/*	*GNU General Public License, version 2*
validator	3.41.2	*http://registry.npmjs.org/validator/-/validator-3.41.2.tgz*	*MIT License*
vary	1.0.1	*http://registry.npmjs.org/vary/-/vary-1.0.1.tgz*	*MIT License*
wanpipe	3.5.18	*http://wiki.sangoma.com/wanpipe-linux-drivers*	*GNU General Public License, version 2*
websocket	2.4	*https://github.com/nori0428/mod_websocket*	*MIT License*
wget	1.14	*http://www.gnu.org/software/wget/*	*GNU General Public License, version 3*
winston	1.0.1	*http://registry.npmjs.org/winston/-/winston-1.0.1.tgz*	*MIT License*
wireless_tools	r29	*http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html*	*GNU General Public License, version 2*
wpa_supplicant	2.0	*http://hostap.epitest.fi/wpa_supplicant/*	*The BSD License*
ws	0.7.2	*http://registry.npmjs.org/ws/-/ws-0.7.2.tgz*	*MIT License*
wuftpd	1.0.21	*http://wu-ftpd.therockgarden.ca/*	*WU-FTPD Software License*
XenAPI	None	*http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html*	*GNU General Public License, version 2*

Name	Version	URL	License
xen	4.1.5	*http://www.xen.org/*	*GNU General Public License, version 2*
xen-crashdump-analyser	20130505	*http://xenbits.xen.org/people/andrewcoop/*	*GNU General Public License, version 2*
xen-tools	4.2.1	*http://xen-tools.org/software/xen-tools/*	*GNU General Public License, version 2*
xxhashjs	0.1.1	*http://registry.npmjs.org/xxhashjs/-/xxhashjs-0.1.1.tgz*	*MIT License*
z3c-rml	2.7.2	*http://pypi.python.org/pypi/z3c.rml*	*Zope Public License (ZPL) Version 2.0*
zlib	1.2.8	*http://www.zlib.net/*	*zlib License*
zope-event	4.0.3	*http://pypi.python.org/pypi/zope.event*	*Zope Public License (ZPL) Version 2.0*
zope-interface	4.1.1	*http://pypi.python.org/pypi/zope.interface*	*Zope Public License (ZPL) Version 2.1*
zope-schema	4.4.2	*http://pypi.python.org/pypi/zope.schema*	*Zope Public License (ZPL) Version 2.0*
zwave	0.1	*http://code.google.com/p/open-zwave/*	*GNU Lesser General Public License, version 2.1*

B.3 OSS Licenses

B.3.1 Apache License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

B.3.2 The BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ”AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,

STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B.3.3 Creative Commons Attribution-ShareAlike License, version 3.0

Creative Commons

Attribution-ShareAlike 3.0 Unported

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. REATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

Definitions

1. "Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.

2. "Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License.

3. "Creative Commons Compatible License" means a license that is listed at http://creativecommons.org/compatiblelicenses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.

4. "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.

5. "License Elements" means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

6. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

7. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

8. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

9. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

10. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

11. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

12. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

13. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;

b. to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified.";

c. to Distribute and Publicly Perform the Work including as incorporated in Collections; and,

d. to Distribute and Publicly Perform Adaptations

For the avoidance of doubt:

1. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

2. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,

3. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the *Uniform Resource Identifier* (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.

b. You may Distribute or Publicly Perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction

license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US)); (iv) a Creative Commons Compatible License. If you license the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that license. If you license the Adaptation under the terms of any of the licenses mentioned in (i), (ii) or (iii) (the "Applicable License"), you must comply with the terms of the Applicable License generally and the following provisions: (I) You must include a copy of, or the URI for, the Applicable License with every copy of each Adaptation You Distribute or Publicly Perform; (II) You may not offer or impose any terms on the Adaptation that restrict the terms of the Applicable License or the ability of the recipient of the Adaptation to exercise the rights granted to that recipient under the terms of the Applicable License; (III) You must keep intact all notices that refer to the Applicable License and to the disclaimer of warranties with every copy of the ork as included in the Adaptation You Distribute or Publicly Perform; (IV) when You Distribute or Publicly Perform the Adaptation, You may not impose any effective technological measures on the Adaptation that restrict the ability of a recipient of the Adaptation from You to exercise the rights granted to that recipient under the terms of the Applicable License. This Section 4(b) applies to the Adaptation as incorporated in a Collection, but this does not require the Collection apart from the Adaptation itself to be made subject to the terms of the Applicable License.

c. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv) , consistent with Section 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

d. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation. Licensor agrees that in those jurisdictions (e.g. Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author's honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

5. Representations, Warranties and Disclaimer.

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous.

Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the emainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of he Licensor and You.

The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO

Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.

Creative Commons may be contacted at http://creativecommons.org/.

B.3.4 DropBear License

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2004 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT

HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LibTomCrypt and LibTomMath are written by Tom St Denis, and are .

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen , Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

B.3.5 GNU General Public License, version 2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program

proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

B.3.6 GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

IIf a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted,

regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided

that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only

in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

B.3.7 GNU Lesser General Public License 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away yourfreedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

Creative Commons Legal Code CC0 1.0 Universal CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if

you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

B.3.8 CCO 1.0 Universal

Creative Commons Legal Code

CC0 1.0 Universal

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDELEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights (defined below) upon the creator and subsequent owner(s) (each and all, an "owner") of an original work of authorship and/or a database (each, a "Work").

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works ("Commons") that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the "Affirmer"), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following:

the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work;

moral rights retained by the original author(s) and/or performer(s);

publicity and privacy rights pertaining to a person's image or likeness depicted in a Work;

rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below;

rights protecting the extraction, dissemination, use and reuse of data in a Work;

database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and

other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof.

Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose.

Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the “License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose.

Limitations and Disclaimers.

No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document.

Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law.

Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without limitation any person's Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work.

Affirmer understands and acknowledges that Creative Commons is not a party to this document and has no duty or obligation with respect to this CC0 or use of the Work.

B.3.9 GNU General Public License, version 3

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution andmodification follow.

TERMS AND CONDITIONS

Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case o interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files forthe work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing i not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of echnological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section

7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules andprotocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives

whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise ofights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any

of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE

PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OFSUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

B.3.10 ISC License

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OFTHIS SOFTWARE.

B.3.11 GNU Lesser General Public License, version 3.0

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General PublicLicense, supplemented by the additional permissions listed below.

Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each ofthe following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you

have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

B.3.12 GNU General Public License 2.0

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, thus in effect making the program proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library,and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   The modified work must itself be a software library.

   You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   IIf, a facility in the modified Library, refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer

version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library.

(It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who

receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY

TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

B.3.13 GNU Lesser General Public License, version 2.0

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which wa designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the

library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

* a) The modified work must itself be a software library.

* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other han as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest you rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, s the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by

law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose thatchoice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

B.3.14 GNU Lesser General Public License, version 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away yourfreedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

B.3.15 GNU LESSER GENERAL PUBLIC LICENSE

ERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

B.3.16 MIT License

Permission is hereby granted, without written agreement and without icense or royalty fees, to use, copy, modify, and distribute this software and its documentation for any purpose, provided that the above copyright notice and the following two paragraphs appear in all copies of this software.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE COPYRIGHT HOLDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE COPYRIGHT HOLDER SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE COPYRIGHT HOLDER HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

B.3.17 Mozilla Public License, version 2

Version 2.0

1. Definitions

1.1. Contributor means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. Contributor Versionâ means the combination of the Contributions of others (if any) used by a Contributor and that particular Contribution.

1.3. Contribution means Covered Software of a particular Contributor.

1.4. Covered Software means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. Incompatible With Secondary Licenses means

1. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

2. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. Executable Form means any form of the work other than Source Code Form.

1.7. Larger Work means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. License means this document.

1.9. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. Modifications means any of the following:

1. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

2. any new file in Source Code Form that contains any Covered Software.

1.11. Patent Claims of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. Secondary License means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. Source Code Form means the form of the work preferred for making modifications.

1.14. You (orYour) means an individual or a legal entity exercising rights under this License. For legal entities, You includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

1. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

2. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

1. for any code that a Contributor has removed from Covered Software; or

2. for infringements caused by: (i) Your and any other third partyâ€™s modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

3. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipientsâ€™ rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

1. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

2. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipientsâ€™ rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an â€œas isâ€? basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such partyâ€™s negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/. You may add additional accurate notices of copyright ownership.

Exhibit B - Incompatible With Secondary Licenses Notice

This Source Code Form is Incompatible With Secondary Licenses, as defined by the Mozilla Public License, v. 2.0.

B.3.18 The Open LDAP Public License

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

B.3.19 OpenSSL License

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contac openssl-core@openssl.org

5. Products derived from this software may not be called "OpenSSL" nor may OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes oftware written by Tim Hudson (tjh@cryptsoft.com).

B.3.20 WU-FTPD Software License

WU-FTPD SOFTWARE LICENSE

Use, modification, or redistribution (including distribution of any modified or derived work) in any form, or on any medium, is permitted only if all the following conditions are met:

1. Redistributions qualify as "freeware" or "Open Source Software" under the following terms:

a. Redistributions are made at no charge beyond the reasonable cost of materials and delivery. Where redistribution of this software is as part of a larger package or combined work, this restriction applies only to the costs of materials and delivery of this software, not to any other costs associated with the larger package or combined work.

b. Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means all files included in the original distribution, including all modifications or additions, on a medium and in a form allowing fully working executable programs to be produced.

2. Redistributions of Source Code must retain the copyright notices as they appear in each Source Code file and the COPYRIGHT file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the"Copyright Notice" refers to the following language:

Copyright (c) 1999,2000,2001 WU-FTPD Development Group.

All rights reserved.

Portions Copyright (c) 1980, 1985, 1988, 1989, 1990, 1991, 1993, 1994

The Regents of the University of California.

Portions Copyright (c) 1993, 1994 Washington University in Saint Louis.

Portions Copyright (c) 1996, 1998 Berkeley Software Design, Inc.

Portions Copyright (c) 1998 Sendmail, Inc.

Portions Copyright (c) 1983, 1995, 1996, 1997 Eric P. Allman.

Portions Copyright (c) 1989 Massachusetts Institute of Technology.

Portions Copyright (c) 1997 Stan Barber.

Portions Copyright (c) 1991, 1992, 1993, 1994, 1995, 1996, 1997 Free Software Foundation, Inc.

Portions Copyright (c) 1997 Kent Landfield.

Use and distribution of this software and its source code are governed by the terms and conditions of the WU-FTPD Software License ("LICENSE").

If you did not receive a copy of the license, it may be obtained online at http://www.wu-ftpd.org/license.html

4. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the WU-FTPD Development Group, the Washington University at Saint Louis, Berkeley Software Design, Inc., and their contributors."

5. Neither the name of the WU-FTPD Development Group, nor the names of any copyright holders, nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission. The names "wuftpd" and "wu-ftpd" are trademarks of the WU-FTPD Development Group and the Washington University at Saint Louis.

6. Disclaimer/Limitation of Liability:

THIS SOFTWARE IS PROVIDED BY THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, AND CONTRIBUTORS, "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, OR CONTRIBUTORS, BE LIABLE FOR ANY DIRECT, NDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. USE, MODIFICATION, OR REDISTRIBUTION, OF THIS SOFTWARE IMPLIES ACCEPTANCE OF ALL TERMS AND CONDITIONS OF THIS LICENSE.

B.3.21 zlib License

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org, madler@alumni.caltech.edu

B.3.22 Python License, Version 2 (Python-2.0)

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

------ --

This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSFtrademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

B.3.23 BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive,royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

B.3.24 CNRI OPEN SOURCE LICENSE AGREEMENT (for Python 1.6b1)

IMPORTANT: PLEASE READ THE FOLLOWING AGREEMENT CAREFULLY.

BY CLICKING ON "ACCEPT" WHERE INDICATED BELOW, OR BY COPYING, INSTALLING OR OTHERWISE USING PYTHON 1.6, beta 1 SOFTWARE, YOU ARE DEEMED TO HAVE AGREED TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6, beta 1 software in source or binary form and its associated documentation,as released at the www.python.org Internet site on August 4, 2000 ("Python 1.6b1").

Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6b1 alone or in any derivative version, provided, however, that CNRIs License Agreement is retained in Python 1.6b1, alone or in any derivative version prepared by Licensee.

Alternately, in lieu of CNRIs License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6, beta 1, is made available subject to the terms and conditions in CNR Is License Agreement. This Agreement may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1011. This Agreement may also be obtained from a proxy server on the Internet using the URL:http://hdl.handle.net/1895.22/1011".

In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6b1 or any part thereof, and wants to make the derivative work available to the public as provided herein, then Licensee hereby agrees to indicate in any such work the nature of the modifications made to Python 1.6b1.

CNRI is making Python 1.6b1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6b1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING PYTHON 1.6b1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of Virginia, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6b1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

B.3.25 CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA

OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

B.3.26 Zope Public License (ZPL) Version 2.0

Zope Public License (ZPL) Version 2.0

This software is Copyright (c) Zope Corporation (tm) and Contributors. All rights reserved.

This license has been certified as open source. It has also been designated as GPL compatible by the Free Software Foundation (FSF).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the, following conditions are met:

Redistributions in source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Zope Corporation (tm) must not be used to endorse or promote products derived from this software without prior written permission from Zope Corporation.

The right to distribute this software or to use it for any purpose does not give you the right to use Servicemarks (sm) orTrademarks (tm) of Zope Corporation. Use of them is covered in a separate agreement (see http://www.zope.com/Marks).

If any files are modified, you must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY ZOPE CORPORATION ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZOPE CORPORATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of contributions made by Zope Corporation and many individuals on behalf of Zope Corporation. Specific attributions are listed in the accompanying credits file.

B.3.27 Zope Public License (ZPL) Version 2.1

Zope Public License (ZPL) Version 2.1

A copyright notice accompanies this license document that identifies the copyright holders.

This license has been certified as open source. It has also been designated as GPL compatible by the Free Software Foundation (FSF).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the, following conditions are met:

Redistributions in source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Zope Corporation (tm) must not be used to endorse or promote products derived from this software without prior written permission from Zope Corporation.

The right to distribute this software or to use it for any purpose does not give you the right to use Servicemarks (sm) orTrademarks (tm) of Zope Corporation. Use of them is covered in a separate agreement (see http://www.zope.com/Marks).

If any files are modified, you must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY ZOPE CORPORATION ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZOPE CORPORATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.