

53-1002313-01  
June 2011



# Brocade Mobility RFS4000, RFS6000 and RFS7000

---

## CLI Reference Guide

Supporting software release 5.1.0.0 and later

**BROCADE**

Copyright © 2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCFM, DCX, Fabric OS, FastIron, IronView, NetIron, SAN Health, ServerIron, TurboIron, and Wingspan are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, Extraordinary Networks, MyBrocade, VCS, and VDX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

## Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters  
Brocade Communications Systems, Inc.  
130 Holger Way  
San Jose, CA 95134  
Tel: 1-408-333-8000  
Fax: 1-408-333-8101  
E-mail: [info@brocade.com](mailto:info@brocade.com)

Asia-Pacific Headquarters  
Brocade Communications Systems China HK, Ltd.  
No. 1 Guanghua Road  
Chao Yang District  
Units 2718 and 2818  
Beijing 100020, China  
Tel: +8610 6588 8888  
Fax: +8610 6588 9999  
E-mail: [china-info@brocade.com](mailto:china-info@brocade.com)

European Headquarters  
Brocade Communications Switzerland Sàrl  
Centre Swissair  
Tour B - 4ème étage  
29, Route de l'Aéroport  
Case Postale 105  
CH-1215 Genève 15  
Switzerland  
Tel: +41 22 799 5640  
Fax: +41 22 799 5641  
E-mail: [emea-info@brocade.com](mailto:emea-info@brocade.com)

Asia-Pacific Headquarters  
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)  
Citic Plaza  
No. 233 Tian He Road North  
Unit 1308 - 13th Floor  
Guangzhou, China  
Tel: +8620 3891 2000  
Fax: +8620 3891 2111  
E-mail: [china-info@brocade.com](mailto:china-info@brocade.com)

## Document History

Title	Publication number	Summary of changes	Date
<i>Brocade Mobility RFS4000, RFS6000 and RFS7000 CLI Reference Guide</i>	53-1002313-01	Additions for software version 5.1.0.0	June 2011

# Table of Contents

---

<b>About This Guide</b>	<b>1</b>
Understanding command syntax	3
Product downloads	4
Manuals	4
Additional information	4
<b>Introduction</b>	<b>5</b>
<b>In this chapter</b>	<b>5</b>
Configuration for connecting to a controller using a terminal emulator	5
User credentials	5
Examples in this reference guide	6
<b>CLI overview</b>	<b>6</b>
Command modes	7
<b>Getting context sensitive help</b>	<b>9</b>
<b>Using the no command</b>	<b>11</b>
Basic conventions	11
<b>Using CLI editing features and shortcuts</b>	<b>11</b>
Moving the cursor on the command line	11
Completing a partial command name	12
Command output pagination	13
Creating profiles	13
Change the default profile by creating VLAN 150 and mapping to ge3 physical interface	13
Viewing configured APs	14
Remote administration	14
Configuring Telnet for management access	14
Configuring ssh	16
<b>User Exec Mode Commands</b>	<b>17</b>
<b>In this chapter</b>	<b>17</b>
<b>User exec commands</b>	<b>18</b>
ap-upgrade	19
change-passwd	22
clear	23
clock	26
cluster	27
commit	28
connect	29
crypto	30
disable	40
enable	41
exit	42
help	43
logging	47
mint	48
no	50
page	51
ping	52
revert	53
service	54
show	55

telnet .....	57
terminal .....	58
time-it .....	59
trace-route .....	60
watch .....	61
write .....	62
clrscr .....	63
exit .....	64

**Privileged Exec Mode Commands 65**

<b>In this chapter .....</b>	<b>65</b>
------------------------------	-----------

<b>Privileged Exec Mode Commands .....</b>	<b>67</b>
--	-----------

ap-upgrade .....	69
archive .....	71
boot .....	72
cd .....	73
change-passwd .....	74
clear .....	75
clock .....	78
clrscr .....	79
cluster .....	80
configure .....	81
commit .....	82
connect .....	83
copy .....	84
crypto .....	85
delete .....	95
disable .....	96
diff .....	97
dir .....	98
edit .....	100
enable .....	101
erase .....	102
exit .....	103
format .....	104
halt .....	105
help .....	106
logging .....	110
mkdir .....	111
mint .....	112
more .....	114
no .....	115
page .....	116
ping .....	117
pwd .....	118
reload .....	119
rename .....	120
revert .....	121
rmdir .....	122
self .....	123
service .....	124
show .....	125
telnet .....	127
terminal .....	128
time-it .....	129
tracert .....	130

upgrade .....	131
upgrade-abort .....	132
watch .....	133
write .....	134

## **Global Configuration Commands 135**

<b>In this chapter .....</b>	<b>135</b>
------------------------------	------------

<b>Global Configuration Commands .....</b>	<b>136</b>
--	------------

aaa-policy .....	138
advanced-wips-policy .....	139
association-acl-policy .....	140
auto-provisioning-policy .....	141
br650 .....	142
br6511 .....	143
br6532 .....	144
br71xx .....	145
Captive Portal Mode .....	146
captive-portal .....	147
Captive-Portal-Mode Commands .....	148
access-time .....	149
access-type .....	150
accounting .....	151
connection-mode .....	152
custom-auth .....	153
inactivity-timeout .....	154
server .....	155
simultaneous-users .....	156
terms-agreement .....	157
use .....	158
webpage-location .....	159
webpage .....	160
clear .....	162
critical-resource-policy .....	163
critical-resource-policy .....	164
critical-resource-policy-mode .....	165
monitor .....	166
no .....	167
customize .....	168
device .....	172
device-categorization .....	173
device-categorization .....	174
device-categorization-mode commands .....	175
mark-device .....	176
no .....	177
dhcp-server-policy .....	178
dns-whitelist .....	179
dns-whitelist .....	180
dns-whitelist mode commands .....	181
permit .....	182
no .....	183
do .....	184
end .....	186

event-system-policy .....	187
event-system-policy .....	188
event-system-policy mode commands .....	189
event .....	190
no .....	198
firewall-policy .....	199
help .....	200
host .....	202
igmp-snoop-policy .....	203
ip .....	204
mac .....	205
management-policy .....	206
mint-policy .....	207
nac-list .....	208
nac-list .....	209
nac-list mode .....	210
exclude .....	211
include .....	212
no .....	213
no .....	214
password-encryption .....	216
profile .....	217
radio-qos-policy .....	219
radius-group .....	220
radius-server-policy .....	221
radius-user-pool-policy .....	222
rf-domain .....	223
rf-domain .....	224
rf-domain-mode .....	225
channel-list .....	226
control-vlan .....	227
layout .....	228
rfs4000 .....	229
rfs6000 .....	230
rfs7000 .....	231
role-policy .....	232
self .....	233
service .....	234
show .....	236
smart-rf-policy .....	238
wips-policy .....	239
wlan .....	240
wlan .....	241
wlan-mode commands .....	242
802.11k .....	244
802.11r .....	245
802.11w .....	246
accounting .....	247
acl .....	248
answer-broadcast-probes .....	249
authentication-type .....	250
bridging-mode .....	251
broadcast-dhcp .....	252
broadcast-ssid .....	253

captive-portal-enforcement	254
client-access	255
client-client-communication	256
client-load-balancing	257
data-rates	258
description	261
encryption-type	262
enforce-dhcp	263
ip	264
kerberos	265
motorola-extensions	267
no	268
proxy-arp-mode	269
radius	270
shutdown	271
ssid	272
use	273
vlan	274
vlan-pool-member	275
wep128	276
wep64	277
wireless-client	278
wpa-wpa2	280
wlan-qos-policy	282
write	283

**Common Commands 285**

<b>In this chapter</b>	<b>285</b>
------------------------	------------

<b>Common Commands</b>	<b>285</b>
------------------------	------------

clear	286
commit	287
exit	288
help	289
no	293
show	295
revert	297
service	298
write	317

**Show Commands 319**

<b>In this chapter</b>	<b>319</b>
------------------------	------------

<b>show commands</b>	<b>319</b>
----------------------	------------

show	322
Global Config Mode	322
PRIVILEGE EXEC Mode	323
USER EXEC Mode	324
adoption	326
advanced-wips	328
ap-upgrade	331
boot	332
captive-portal	333
cdp	335

clock	336
cluster	337
commands	338
context	340
critical-resources	342
crypto	343
debug	346
debugging	348
device-categorization	350
event-history	351
event-system-policy	352
file	353
firewall	354
interface	358
ip	360
ip-access-list-stats	364
licenses	365
lldp	366
logging	367
mac-access-list-stats	369
mac-address-table	370
mint	371
noc	373
ntp	376
password-encryption	377
power	378
remote-debug	380
rf-domain-manager	381
role	382
running-config	383
session-changes	385
session-config	386
sessions	387
smart-rf	388
spanning-tree	390
startup-config	393
terminal	394
timezone	395
upgrade-status	396
version	397
wireless	398
wwan	405

**Profiles 407**

**In this chapter 407**

**Creating profiles 408**

aaa	410
arp	412
auto-learn-staging-config	414
autoinstall	415
ap-upgrade	416
bridge commands	417
bridge	418
bridge-vlan mode commands	419
bridging-mode	420



description .....	421
edge-vlan .....	422
ip .....	423
no .....	425
stateful-packet-inspection-12 .....	426
use .....	427
cdp .....	428
cluster .....	429
configuration-persistence .....	431
controller .....	432
crypto .....	434
isakmp-policy .....	438
authentication .....	439
encryption .....	440
group .....	441
hash .....	442
life-time .....	443
no .....	444
crypto-group .....	445
dns .....	446
wns .....	447
dscp-mapping .....	448
email-notification .....	450
enforce-version .....	452
events .....	454
ip .....	455
nat-pool .....	459
address .....	460
no .....	461
interface .....	462
Interface Config Instance .....	464
cdp .....	466
channel-group .....	467
description .....	468
dot1x .....	469
duplex .....	470
ip .....	471
lldp .....	472
no .....	473
power .....	474
qos .....	475
shutdown .....	476
spanning-tree .....	477
speed .....	480
switchport .....	481
use .....	483
Interface vlan Instance .....	484
crypto .....	485
description .....	486
dhcp-relay-incoming .....	487
ip .....	488
no .....	489
shutdown .....	490
use .....	491

led	492
legacy-auto-downgrade	493
legacy-auto-update	494
lldp	495
load-balancing	496
local	498
logging	499
mac-address-table	501
mint	502
misconfiguration-recovery-time	505
monitor	506
neighbor-inactivity-timeout	507
neighbor-info-interval	508
no	509
noc	510
ntp	511
preferred-controller-group	512
power-config	513
radius	514
rf-domain-manager	515
service	516
spanning-tree	517
use	520
vpn	522
wep-shared-key-auth	523

**Device specific commands** ..... **524**

ap-upgrade	525
area	526
contact	527
country-code	528
dhcp-redundancy	529
floor	530
hostname	531
layout-coordinates	532
location	533
mac-name	534
neighbor-info-interval	535
override-wlan	536
remove-override	537
rsa-key	538
sensor-server	539
stats	540
timezone	541
trustpoint	542
wwan	543

**aaa-policy** ..... **545**

**In this chapter** ..... **545**

**aaa-policy** ..... **546**

accounting	547
authentication	551
mac-address-format	555
no	556
server-pooling-mode	557
use	558

write	559
clrscr	561
commit	562
do	563
end	565
exit	566
health-check	567
help	568
revert	569
service	570
show	572
<b>auto-provisioning-policy</b>	<b>575</b>
<b>In this chapter</b>	<b>575</b>
<b>auto-provisioning-policy</b>	<b>576</b>
adopt	577
default-adoption	580
deny	581
no	583
<b>advanced-wips-policy</b>	<b>585</b>
<b>In this chapter</b>	<b>585</b>
<b>advanced-wips-policy</b>	<b>585</b>
event	587
no	592
server-listen-port	593
terminate	594
use	595
<b>association-acl-policy</b>	<b>597</b>
<b>In this chapter</b>	<b>597</b>
<b>association-acl-policy</b>	<b>597</b>
deny	598
no	599
permit	600
<b>access-list</b>	<b>601</b>
<b>In this chapter</b>	<b>601</b>
<b>ip-access-list</b>	<b>602</b>
deny	603
permit	608
no	613
write	614
clrscr	616
commit	617
end	618
exit	619
help	620
revert	621
service	622
show	624

<b>mac-access-list</b> .....	<b>625</b>
permit .....	626
deny .....	632
<b>dhcp-server-policy</b> .....	<b>637</b>
<b>In this chapter</b> .....	<b>637</b>
<b>dhcp-server-policy</b> .....	<b>638</b>
bootp .....	639
dhcp-pool .....	640
dhcp-pool mode .....	641
address .....	642
bootfile .....	643
ddns .....	644
default-router .....	645
dns-server .....	646
domain-name .....	647
excluded-address .....	648
lease .....	649
netbios-name-server .....	651
netbios-node-type .....	652
next-server .....	653
no .....	654
option .....	655
respond-via-unicast .....	656
update .....	657
static-binding .....	658
static-binding mode .....	660
bootfile .....	661
client-name .....	662
default-router .....	663
dns-server .....	664
domain-name .....	665
ip-address .....	666
netbios-name-server .....	667
netbios-node-type .....	668
next-server .....	669
no .....	670
option .....	671
respond-via-unicast .....	672
static-route .....	673
option .....	674
no .....	675
ping .....	676
dhcp-class .....	677
dhcp-class mode .....	678
multiple-user-class .....	679
no .....	680
option .....	681
<b>firewall-policy</b> .....	<b>683</b>
<b>In this chapter</b> .....	<b>683</b>

<b>firewall-policy</b> .....	<b>684</b>
alg .....	685
clamp .....	686
dhcp-offer-convert .....	687
dns-snoop .....	688
firewall .....	689
flow .....	690
ip .....	692
ip-mac .....	695
logging .....	696
no .....	697
proxy-arp .....	698
stateful-packet-inspection-12 .....	699
storm-control .....	700
virtual-defragmentation .....	702
<b>igmp-snoop-policy</b> .....	<b>703</b>
<b>In this chapter</b> .....	<b>703</b>
<b>igmp-snoop-policy</b> .....	<b>703</b>
igmp-snooping .....	704
querier .....	705
robustness-variable .....	706
unknown-multicast-fwd .....	707
no .....	708
<b>mint-policy</b> .....	<b>709</b>
<b>In this chapter</b> .....	<b>709</b>
<b>mint-policy</b> .....	<b>710</b>
level .....	711
mtu .....	712
re-join timeout .....	713
security-level .....	714
sign-unknown-device .....	715
udp .....	716
no .....	717
<b>management-policy</b> .....	<b>719</b>
<b>In this chapter</b> .....	<b>719</b>
<b>management-policy</b> .....	<b>720</b>
aaa-login .....	721
banner .....	723
ftp .....	724
http .....	726
https .....	727
no .....	728
restrict-access .....	729
snmp-server .....	730
ssh .....	733
telnet .....	734
user .....	735
<b>radius-policy</b> .....	<b>737</b>

<b>In this chapter</b> .....	<b>737</b>
<b>radius-group</b> .....	<b>738</b>
guest .....	739
policy .....	740
rate-limit .....	742
no .....	743
<b>radius-server-policy</b> .....	<b>744</b>
authentication .....	745
crl-check .....	746
ldap-group-verification .....	747
ldap-server .....	748
local .....	750
nas .....	751
no .....	752
proxy .....	753
session-resumption .....	754
use .....	755
<b>radius-user-pool-policy</b> .....	<b>756</b>
user .....	757
no .....	758
<b>radio-qos-policy</b> .....	<b>759</b>
<b>In this chapter</b> .....	<b>759</b>
<b>radio-qos-policy</b> .....	<b>759</b>
accelerated-multicast .....	760
admission-control .....	761
no .....	763
wmm .....	764
<b>role-policy</b> .....	<b>767</b>
<b>In this chapter</b> .....	<b>767</b>
<b>role-policy</b> .....	<b>767</b>
default-role .....	768
no .....	769
user-role .....	770
ap-location .....	771
authentication-type .....	772
captive-portal .....	773
encryption-type .....	774
group .....	775
mu-mac .....	776
no .....	777
ssid .....	778
use .....	779
<b>smart-rf-policy</b> .....	<b>781</b>
<b>In this chapter</b> .....	<b>781</b>
<b>smart-rf-policy</b> .....	<b>782</b>
assignable-power .....	783
auto-assign-sensor .....	784

channel-list .....	785
channel-width .....	786
coverage-hole-recovery .....	787
enable .....	788
group-by .....	789
interference-recovery .....	790
neighbor-recovery .....	791
no .....	792
sensitivity .....	793
smart-ocs-monitoring .....	794
<b>wips-policy .....</b>	<b>795</b>
<b>In this chapter .....</b>	<b>795</b>
<b>wips-policy .....</b>	<b>796</b>
ap-detection .....	797
enable .....	798
event .....	799
history-throttle-duration .....	802
no .....	803
use .....	804
signature .....	805
bssid .....	807
dst-mac .....	808
filter-ageout .....	809
frame-type .....	810
mode .....	811
payload .....	812
src-mac .....	813
ssid-match .....	814
threshold-client .....	815
threshold-radio .....	816
no .....	817
<b>wlan-qos-policy .....</b>	<b>819</b>
<b>In this chapter .....</b>	<b>819</b>
<b>wlan-qos-policy .....</b>	<b>820</b>
accelerated-multicast .....	821
classification .....	822
multicast-mask .....	823
no .....	824
qos .....	825
rate-limit .....	826
svp-prioritization .....	828
voice-prioritization .....	829
wmm .....	830
<b>interface-radio Commands .....</b>	<b>833</b>
<b>In this chapter .....</b>	<b>833</b>
<b>interface-radio Instance .....</b>	<b>834</b>
ack-timeout .....	836
aggregation .....	837
airtime-fairness .....	838

antenna-diversity	839
antenna-gain	840
antenna-mode	841
beacon	842
channel	843
data-rates	844
description	846
dynamic-chain-selection	847
guard-interval	848
lock-rf-mode	849
max-clients	850
mesh	851
no	852
non-unicast	853
off-channel-scan	854
placement	855
power	856
preamble-short	857
probe-response	858
radio-share-mode	859
rf-mode	860
rifs	861
rts-threshold	862
shutdown	863
sniffer-redirect	864
use	865
wlan	866
wireless-client	868

**Firewall Logging 869**

**In this chapter 869**

**Firewall Log Terminology and Syslog Severity Levels 869**

Date format in Syslog messages	870
FTP data connection log	870
The FTP connection is Control Connection	870
The Data Connection in Active Mode	871
The Data Connection in Passive Mode	871
UDP packets log	871
DHCP Release	871
DHCP Renew	871
ICMP type logs	872
ICMP type logs	872
Raw IP Protocol logs	873
Raw IP Protocol logs	874
Firewall startup log	874
Manual time change log	875
Firewall ruleset log	875
IP ACL IN on WLAN Attach	875
IP ACL IN on WLAN Remove	876
IP ACL OUT on WLAN Attach	876
IP ACL OUT on WLAN Remove	876
MAC ACL IN on WLAN Attach	876
MAC ACL IN on WLAN Remove	876



MAC ACL OUT on WLAN Attach .....	876
MAC ACL OUT on WLAN Remove .....	876
IP ACL on VLAN Attach.....	876
IP ACL on VLAN Remove .....	876
IP ACL on GE Port Attach .....	876
IP ACL on GE Port Remove .....	877
MAC ACL on GE Port Attach.....	877
MAC ACL on GE Port Remove .....	877
IP ACL on Port-Channel Attach .....	877
IP ACL on Port-Channel Remove .....	877
MAC ACL on Port-Channel Attach .....	877
MAC ACL on Port-Channel Remove.....	877
Rule added / deleted from IP/MAC ACL.....	877
TCP Reset Packets log .....	877
ICMP Destination log .....	878
ICMP Packet log .....	878
SSH connection log .....	878
Allowed/Dropped Packets Log .....	879
Allow Packets .....	879
Drop/Deny Packets .....	879



# About This Guide

---

## In this chapter

- [Document set](#) ..... 1
- [Document convention](#) ..... 2
- [Notational conventions](#) ..... 2
- [Web support sites](#) ..... 4

This guide provides information on using the following Brocade wireless controllers and access points:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

## Document set

The documentation set for the Brocade wireless controllers is partitioned into the following guides to provide information for specific user deployment requirements.

- *Installation Guides* - Each controller has a unique Installation Guide which describes the basic hardware setup and configuration required to transition to more advanced configuration
- *Brocade Mobility RFS4000, RFS6000 and RFS7000 System Reference Guide* - Describes configuration of the Brocade wireless controllers using the Web UI.
- *Brocade Mobility RFS4000, RFS6000 and RFS7000 CLI Reference Guide* (this document) - Describes the *Command Line Interface* (CLI) and *Management Information Base* (MIB) commands used to configure the Brocade wireless controllers.

## Document convention

The following conventions are used in this document to draw your attention to important information:

---

**NOTE**

Indicates tips or special requirements.

---

**CAUTION**

Indicates conditions that can cause equipment damage or data loss.

---

**DANGER**

**Indicates a condition or procedure that could result in personal injury or equipment damage.**

---

## Notational conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
- Bullets (•) indicate:
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
  - action items
- Sequential lists (those describing step-by-step procedures) appear as numbered lists

## Understanding command syntax

---

<variable>

Variables are described with a short description enclosed within a '<' and a '>' pair.

For example, the command,

```
RFController>show interface ge 1
```

is documented as

```
show interface ge <idx>
```

- show – The command – Display information
- interface – The keyword – The interface
- <idx> – The variable – ge Index value

---

|

The pipe symbol. This is used to separate the variables/keywords in a list.

For example, the command

```
RFController> show .....
```

is documented as

```
show
```

```
[adoption|advanced-wips|boot|captive-portal|.....]
```

where:

- show – The command
- [adoption|advanced-wips|boot|captive-portal|.....] – Indicates the different commands that can be combined with the show command. However, only one of the above list can be used at a time.

```
show adoption ...
```

```
show advanced-wips ...
```

```
show boot ...
```

---

[]

Of the different keywords and variables listed inside a '[' & ']' pair, only one can be used. Each choice in the list is separated with a '|' (pipe) symbol.

For example, the command

```
RFController# clear ...
```

is documented as

```
clear [arp-cache|cdp|crypto|event-history|
```

```
firewall|ip|spanning-tree]
```

where:

- clear – The command
- [arp-cache|cdp|crypto|event-history|firewall|ip|spanning-tree] – Indicates that seven keywords are available for this command and only one can be used at a time

---

{ }	<p>Any command/keyword/variable or a combination of them inside a '{ &amp; }' pair is optional. All optional commands follow the same conventions as listed above. However they are displayed italicized.</p> <p>For example, the command</p> <pre>RFController&gt; show adoption ....</pre> <p>is documented as</p> <pre>show adoption info {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</pre> <p>Here:</p> <ul style="list-style-type: none"> <li>• show adoption info – The command. This command can also be used as <code>show adoption info</code></li> <li>• {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – The optional keyword <code>on</code> &lt;device-or-domain-name&gt;. The command can also be extended as <code>show adoption info {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}</code></li> </ul> <p>Here the keyword {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} is optional.</p>
command / keyword	<p>The first word is always a command. Keywords are words that must be entered as is. Commands and keywords are mandatory.</p> <p>For example, the command,</p> <pre>RFController&gt;show wireless</pre> <p>is documented as</p> <pre>show wireless</pre> <p>where:</p> <ul style="list-style-type: none"> <li>• show – The command</li> <li>• wireless – The keyword</li> </ul>

---

## Web support sites

### Product downloads

<http://www.brocade.com>

### Manuals

<http://www.brocade.com/ethernetproducts>

### Additional information

<http://www.brocade.com>

# Introduction

---

## In this chapter

- [CLI overview](#) ..... 6
- [Getting context sensitive help](#) ..... 9
- [Using the no command](#) ..... 11
- [Using CLI editing features and shortcuts](#) ..... 11

This chapter describes the commands available using the controller *Command Line Interface* (CLI) on a Brocade device. The CLI is available for all supported devices, controllers as well as Access Points (APs).

Access the CLI by:

- A terminal emulation program running on a computer connected to the serial port on the controller. The serial port is located on the front of the controller.
- A Telnet session through *Secure Shell* (SSH) over a network.

## Configuration for connecting to a controller using a terminal emulator

If connecting through the serial port, use the following settings to configure your terminal emulator:

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	None

When a CLI session is established, complete the following (user input is in *bold*):

```
login as: admin
administrator's login password: admin123
```

## User credentials

Use the following credentials when logging into a device for the first time:

User Name	admin
Password	admin123

When logging into the CLI for the first time, you are prompted to change the password.

## Examples in this reference guide

Examples used in this reference guide are generic to the each supported controller model and AP. Commands that are not common, are identified using the notation “Supported in the following platforms.” For an example, see below:

Supported In the following platforms:

Mobility RFS6000 Controller

The above example indicates the command is only available on a Mobility RFS6000 Controller model controller.

## CLI overview

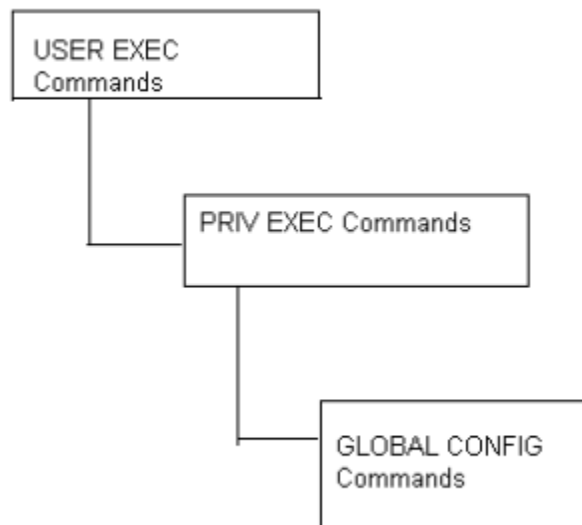
The CLI is used for configuring, monitoring, and maintaining the controller managed network. The user interface allows you to execute commands on supported controllers and AP models, using either a serial console or a remote access method.

This chapter describes basic CLI features. Topics covered include an introduction to command modes, navigation and editing features, help features and command history.

The CLI is segregated into different command modes. Each mode has its own set of commands for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in, and to a lesser extent, the particular model used. Enter a question mark (?) at the system prompt to view a list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is: USER EXEC mode, PRIV EXEC mode and GLOBAL CONFIG mode.

**FIGURE 1** Hierarchy of User Modes





## Command modes

A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode). For security, only a limited subset of EXEC commands are available in the USER EXEC mode. This level is reserved for tasks that do not change the controller configuration.

```
RFController>
```

The system prompt signifies the device name and the last three bytes of the device MAC address.

To access commands, enter the PRIV EXEC mode (the second access level for the EXEC mode). Once in the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

```
RFController> enable
RFController#
```

Most of the USER EXEC mode commands are one-time commands and are not saved across controller reboots. Save the command by executing 'commit' command. For example, the show command displays the current configuration and the clear command clears the interface.

Access the GLOBAL CONFIG mode from the PRIV EXEC mode. In the GLOBAL CONFIG mode, enter commands that set general system characteristics. Configuration modes, allow you to change the running configuration. If you save the configuration later, these commands are stored across controller reboots.

Access a variety of protocol specific (or feature-specific) modes from the global configuration mode. The CLI hierarchy requires you to access specific configuration modes only through the global configuration mode.

```
RFController# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RFController(config)#
```

You can also access sub-modes from the global configuration mode. Configuration sub-modes define specific features within the context of a configuration mode.

```
RFController(config)# aaa-policy test
RFController(config-aaa-policy-test)#
```

Table 1 Summarizes available controller commands.

**TABLE 1** All Modes Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
ap-upgrade	ap-upgrade	aaa-policy
change-passwd	archive	advanced-wips-policy
clear	boot	br650
clock	cd	br6511
cluster	change-passwd	br6532
commit	clear	br7131
connect	clock	association-acl-policy
crypto	cluster	auto-provisioning-policy
debug	commit	captive-portal
disable	configure	clear
enable	connect	critical-resource-policy
help	copy	customize
logging	crypto	device
mint	debug	device-categorization
no	delete	dhcp-server-policy
page	diff	dns-whitelist
ping	dir	event-system-policy
remote-debug	disable	firewall-policy
revert	edit	help
service	enable	host
show	erase	igmp-snoop-policy
telnet	format	ip
terminal	halt	mac
time-it	help	management-policy
traceroute	logging	mint-policy
watch	mint	nac-list
write	mkdir	no
clrscr	more	password-encryption
exit	no	profile
	page	radio-qos-policy
	ping	radius-group
	pwd	radius-server-policy
	reload	radius-user-pool-policy
	remote-debug	rf-domain
	rename	rfs4000

**TABLE 1** All Modes Commands

User Exec Mode	Priv Exec Mode	Global Configuration Mode
	revert	rfs6000
	rmdir	rfs7000
	self	role-policy
	service	self
	show	smart-rf-policy
	telnet	wips-policy
	terminal	wlan
	time-it	wlan-qos-policy
	traceroute	write
	upgrade	clrscr
	upgrade-abort	commit
	watch	do
	write	end
	clrscr	exit
	exit	revert
		show

## Getting context sensitive help

Enter a question mark (?) at the system prompt to display a list of commands available for each mode. Obtain a list of arguments and keywords for any command using the CLI context-sensitive help.

Use the following commands to obtain help specific to a command mode, command name, keyword or argument:

Command	Description
(prompt)# help	Displays a brief description of the help system
(prompt)# abbreviated-command-entry?	Lists commands in the current mode that begin with a particular character string
(prompt)# abbreviated-command-entry<Tab>	Completes a partial command name
(prompt)# ?	Lists all commands available in the command mode
(prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command
(prompt)# command keyword ?	Lists the next available syntax option for the command

### NOTE

Enter Ctrl + V to use ? as a regular character and not as a character used for displaying context sensitive help. This is required when the user has to enter a URL that ends with a?

---

**NOTE**

The escape character used through out the CLI is “\”. To enter a “\” use “\\” instead.

---

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular sequence, enter the characters followed by a question mark (?). Do not include a space. This form of help is called word help, because it completes a word.

```
RFController#service?  
service Service Commands  
RFController#service
```

Enter a question mark (?) (in place of a keyword or argument) to list keywords or arguments. Include a space before the ?. This form of help is called command syntax help. It shows the keywords or arguments available based on the command/keyword and argument already entered.

```
RFController>service ?  
advanced-wips      Advanced WIPS service commands  
clear              Clear  
cli-tables-expand  Expand the cli-table in drapdown format  
cli-tables-skin    Choose a formatting layout/skin for CLI tabular outputs  
cluster            Cluster Protocol  
locator            Enable leds flashing on the device  
pktcap             Start packet capture  
radio              Radio parameters  
show               Show running system information  
smart-rf           Smart-RF Management Commands  
traceroute         Trace route to destination  
wireless           Wireless commands  
RFController>service
```

It's possible to abbreviate commands and keywords to allow a unique abbreviation. For example, “configure terminal” can be abbreviated as `config t`. Since the abbreviated command is unique, the controller accepts the abbreviation and executes the command.

Enter the help command (available in any command mode) to provide the following description:

```
RFController>help  
CLI provides advanced help feature.  When you need help,  
anytime at the command line please press '?'.  
  
If nothing matches, the help list will be empty and you must backup  
until entering a '?' shows the available options.  
Two styles of help are provided:  
1. Full help is available when you are ready to enter a  
command argument (e.g. 'show ?') and describes each possible  
argument.  
2. Partial help is provided when an abbreviated argument is entered and you  
want to know what arguments match the input  
(e.g. 'show ve?'.)
```

## Using the no command

Almost every command has a `no` form. Use `no` to disable a feature or function or return it to its default value. Use the command without the `no` keyword to re-enable a disabled feature.

### Basic conventions

Keep the following conventions in mind while working within the controller CLI:

- Use `?` at the end of a command to display available sub-modes. Type the first few characters of the sub-mode and press the tab key to add the sub-mode. Continue using `?` until you reach the last sub-mode.
- Pre-defined CLI commands and keywords are case-insensitive: `cfg` = `Cfg` = `CFG`. However (for clarity), CLI commands and keywords are displayed (in this guide) using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`.
- Enter commands in uppercase, lowercase, or mixed case. Only passwords are case sensitive.

## Using CLI editing features and shortcuts

A variety of shortcuts and edit features are available. The following describe these features:

- [Moving the cursor on the command line](#)
- [Completing a partial command name](#)
- [Command output pagination](#)

### Moving the cursor on the command line

[Table 2](#) on page 11 Shows the key combinations or sequences to move the command line cursor. Ctrl defines the control key, which must be pressed simultaneously with its associated letter key.

Esc means the escape key (which must be pressed first), followed by its associated letter key. Keys are not case sensitive. Specific letters are used to provide an easy way of remembering their functions. In [Table 2](#) on page 11, bold characters indicate the relation between a letter and its function.

**TABLE 2** Keystrokes Details

Keystrokes	Function Summary	Function Details
Left Arrow or Ctrl-B	Back character	Moves the cursor one character to the left When entering a command that extends beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to move back to the system prompt.
Right Arrow or Ctrl-F	Forward character	Moves the cursor one character to the right
Esc- B	Back word	Moves the cursor back one word
Esc- F	Forward word	Moves the cursor forward one word
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the command line
Ctrl-E	End of line	Moves the cursor to the end of the command line
Ctrl-D		Deletes the current character

**TABLE 2** Keystrokes Details

Keystrokes	Function Summary	Function Details
Ctrl-U		Deletes text up to cursor
Ctrl-K		Deletes from the cursor to end of the line
Ctrl-P		Obtains the prior command from memory
Ctrl-N		Obtains the next command from memory
Esc-C		Converts the letter at the cursor to uppercase
Esc-L		Converts the letter at the cursor to lowercase
Esc-D		Deletes the remainder of a word
Ctrl-W		Deletes the word up to the cursor
Ctrl-Z		Returns to the root prompt
Ctrl-T		Transposes the character to the left of the cursor with the character located at the cursor.
Ctrl-L		Clears the screen

## Completing a partial command name

If you cannot remember a command name (or if you want to reduce the amount of typing you have to perform), enter the first few letters of a command, then press the Tab key. The command line parser completes the command if the string entered is unique to the command mode. If your keyboard does not have a Tab key, press Ctrl-L.

The CLI recognizes a command once you have entered enough characters to make the command unique. If you enter “conf” within the privileged EXEC mode, the CLI associates the entry with the configure command, since only the configure command begins with `conf`.

In the following example, the CLI recognizes a unique string in the privileged EXEC mode when the Tab key is pressed:

```
RFController# conf<Tab>
RFController# configure
```

When using the command completion feature, the CLI displays the full command name. The command is not executed until the Return or Enter key is pressed. Modify the command if the full command was not what you intended in the abbreviation. If entering a set of characters (indicating more than one command), the system lists all commands beginning with that set of characters.

Enter a question mark (?) to obtain a list of commands beginning with that set of characters. Do not leave a space between the last letter and the question mark (?).

For example, entering U lists all commands available in the current command mode:

```
RFController# co?
commit      Commit all changes made in this session
configure   Enter configuration mode
connect     Open a console connection to a remote device
copy        Copy from one file to another
RFController# co
```

**NOTE**

The characters entered before the question mark are reprinted to the screen to complete the command entry.

## Command output pagination

Output often extends beyond the visible screen length. For cases where output continues beyond the screen, the output is paused and a

```
--More--
```

prompt displays at the bottom of the screen. To resume the output, press the Enter key to scroll down one line or press the Spacebar to display the next full screen of output.

## Creating profiles

Profiles are sort of a 'template' representation of configuration. The system has a couple of default profiles including:

- a default controller profile
- a default Mobility 7131 Series Access Point profile

To modify the default controller profile to assign an IP address to the management port:

```
RFController(config)#profile rfs7000 default-rfs-7000
RFController(config-profile-default-rfs-7000)#interface me1
RFController(config-profile-default-rfs-7000-if-me1)#ip address
172.16.10.2/24
RFController(config-profile-default-rfs-7000-if-me1)#commit
RFController(config-profile-default-rfs-7000)#exit
RFController(config)#
```

The following command displays default br7131 profile:

```
RFController(config)#profile br7131 defalut-br7131
RFController(config-profile-defalut-br7131)#show context
```

## Change the default profile by creating VLAN 150 and mapping to ge3 physical interface

Logon to the controller in config mode and follow the procedure below:

```
RFController(config-profile-default-rfs7000)# interface vlan 150
RFController(config-profile-default-rfs7000-if-vlan150)# ip address
192.168.150.20/24
RFController(config-profile-default-rfs7000-if-vlan150)# exit
RFController(config-profile-default-rfs7000)# interface ge 3
RFController(config-profile-default-rfs7000-if-ge3)# switchport access vlan
150
RFController(config-profile-default-rfs7000-if-ge3)# commit write
[OK]
RFController(config-profile-default-rfs7000-if-ge3)# show interface vlan 150
Interface vlan150 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 8, Metric: 1, MTU: 1500
  IP-Address: 192.168.150.20/24
```

## 2 Using CLI editing features and shortcuts

```
input packets 43, bytes 12828, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 0, bytes 0, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

### *Viewing configured APs*

To view previously configured APs, enter the following command:

```
RFController(config)#show wireless ap configured
```

## Remote administration

A terminal server may function in remote administration mode if either the terminal services role is not installed on the machine or the client used to invoke the session has enabled the admin controller.

- A terminal emulation program running on a computer connected to the serial port on the controller. The serial port is located on the front of the controller.
- A Telnet session through a *Secure Shell* (SSH) over a network. The Telnet session may or may not use SSH depending on how the wireless controller is configured. Brocade recommends using SSH for remote administration tasks.

### *Configuring Telnet for management access*

Login through the serial console. Perform the following:

1. A session generally begins in the USER EXEC mode (one of the two access levels of the EXEC mode).
2. Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

```
RFController> en
RFController# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

3. Go to 'default-management-policy' mode.

```
RFController(config)# management-policy ?
RFController(config)# management-policy default
RFController(config-management-policy-default)#
```

4. Enter Telnet and the port number at the command prompt. The port number is optional. The default port is 23. Commit the changes after every command. Telnet is enabled.

```
RFController(config-management-policy-default)# telnet
RFController(config-management-policy-default)# commit write
```

5. Use the following credentials when logging on to the device for the first time

User Name	admin
Password	admin123

When logging into the controller for the first time, you are prompted to change the password.

To change user credentials, perform the following:



1. Enter the username, password, role and access details

```

RFController(config-management-policy-default)# user testuser password brocade
role helpdesk access all ?
RFController(config-management-policy-default)# user testuser password brocade
role helpdesk access all
RFController(config-management-policy-default)# commit
RFController(config-management-policy-default)# show context
management-policy default
telnet
http server
ssh
user admin password 1
c9745a77bb8663fbe9422c0bab93087208e68c40add8edd0a3b4a985aa96a682 role
superuser access all
user testuser password 1
fd6af6a0e74ede3fc4bd54519e4864b078554aa2d97a623eedefae2ede682c13 role
helpdesk access all
RFController(config-management-policy-default)# show con
RFController(config-management-policy-default)# show conin
RFController(config-management-policy-default)# show context include-factory
management-policy default
secure-management
telnet port 23
http server
no https server
no ftp
ssh port 22
user admin password 1
c9745a77bb8663fbe9422c0bab93087208e68c40add8edd0a3b4a985aa96a682 role
superuser access all
user testuser password 1
fd6af6a0e74ede3fc4bd54519e4864b078554aa2d97a623eedefae2ede682c13 role
helpdesk access all
snmp-server manager v2
snmp-server manager v3
no snmp-server enable traps
RFController(config-management-policy-default)#

```

2. Logon to the Telnet console and provide the user details configured in the previous step to access the controller

```

RFS7000 release 5.1.0.0-070D
RFController login: testuser
Password:
Welcome to CLI
Starting CLI...
RFController>

```

### *Configuring ssh*

By default, SSH is enabled on the controller. The controller requires an IP address and login credentials.

To enable SSH access in the default profile, login through the serial console. Perform the following steps:

1. Access the GLOBAL CONFIG mode from the PRIV EXEC mode.

```
RFController> en
RFController# configure
Enter configuration commands, one per line. End with CNTL/Z.
```

2. Go to 'default-management-policy' mode.

```
RFController(config)# management-policy default
RFController(config-management-policy-default)#
```

3. Enter ssh at the command prompt.

```
RFController(config-management-policy-default)# ssh
```

4. Login to the wireless controller through SSH using appropriate credentials.
5. Use the following credentials when logging on to the device for the first time

User Name	admin
Password	admin123

On logging into the controller for the first time, you are prompted to change the password.

# User Exec Mode Commands

---

## In this chapter

- [User exec commands](#) ..... 18

Logging in to the controller places you within the USER EXEC command mode. Typically, a login requires a user name and password. You have three login attempts before the connection attempt is refused. USER EXEC commands (available at the user level) are a subset of the commands available at the privileged level. In general, USER EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use `?` at the command prompt. The USER EXEC prompt consists of the device host name followed by an angle bracket (`>`).

```
RFController>?
User Exec commands:
  ap-upgrade      AP firmware upgrade
  change-passwd   Change password
  clear           Clear
  clock           Configure software system clock
  cluster         Cluster commands
  commit          Commit all changes made in this session
  connect         Open a console connection to a remote device
  crypto          Encryption related commands
  debug           Debugging functions
  disable         Turn off privileged mode command
  enable          Turn on privileged mode command
  help            Description of the interactive help system
  logging         Modify message logging facilities
  mint            MiNT protocol
  no              Negate a command or set its defaults
  page           Toggle paging
  ping           Send ICMP echo messages
  remote-debug    Troubleshoot remote system(s)
  revert          Revert changes
  service         Service Commands
  show            Show running system information
  telnet         Open a telnet connection
  terminal        Set terminal line parameters
  watch          Repeat the specific CLI command at a periodic interval
  write          Write running configuration to memory or terminal

  clrscr         Clears the display screen
  exit           Exit from the CLI

RFController>
```

## User exec commands

Table 3 Summarizes User Exec Mode Commands

**TABLE 3** User Exec Commands

Command	Description	Reference
<a href="#">ap-upgrade</a>	Enables an automatic adopted AP firmware upgrade	<a href="#">page 19</a>
<a href="#">change-passwd</a>	Changes the password of a logged user	<a href="#">page 22</a>
<a href="#">clear</a>	Resets the last saved command	<a href="#">page 23</a>
<a href="#">clock</a>	Configures the system clock	<a href="#">page 26</a>
<a href="#">cluster</a>	Accesses the cluster context	<a href="#">page 27</a>
<a href="#">commit</a>	Commits all the updates in the active session	<a href="#">page 28</a>
<a href="#">connect</a>	Establishes a console connection to a remote device	<a href="#">page 29</a>
<a href="#">crypto</a>	Enables encryption	<a href="#">page 30</a>
<a href="#">disable</a>	Turns off (disables) the privileged mode command set	<a href="#">page 40</a>
<a href="#">enable</a>	Turns on (enables) the privileged mode command set	<a href="#">page 41</a>
<a href="#">help</a>	Displays the interactive help system	<a href="#">page 43</a>
<a href="#">logging</a>	Modifies message logging facilities	<a href="#">page 47</a>
<a href="#">mint</a>	Configures the MiNT protocol	<a href="#">page 48</a>
<a href="#">no</a>	Negates a command or sets its default value	<a href="#">page 50</a>
<a href="#">page</a>	Toggles to the controller paging function	<a href="#">page 51</a>
<a href="#">ping</a>	Sends ICMP echo messages to a user-specified location	<a href="#">page 52</a>
<a href="#">revert</a>	Reverts the changes made in the active session to their last configuration	<a href="#">page 53</a>
<a href="#">show</a>	Displays the settings for the specified system component	<a href="#">page 55</a>
<a href="#">telnet</a>	Opens a Telnet session	<a href="#">page 57</a>
<a href="#">terminal</a>	Sets the length/number of lines displayed within the terminal window	<a href="#">page 58</a>
<a href="#">time-it</a>	Verifies the time taken by a particular command between request and response	<a href="#">page 59</a>
<a href="#">trace-route</a>	Traces the route to its defined destination	<a href="#">page 60</a>
<a href="#">watch</a>	Repeats the specific CLI command at a periodic interval	<a href="#">page 61</a>
<a href="#">write</a>	Writes the system running configuration to memory or terminal	<a href="#">page 62</a>
<a href="#">clrscr</a>	Clears the screen	<a href="#">page 63</a>
<a href="#">exit</a>	Ends the current mode and moves to the previous mode	<a href="#">page 64</a>

## ap-upgrade

### *User exec commands*

Enables an automatic adopted AP firmware upgrade

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```

ap-upgrade
[<DEVICE-NAME> | all | br650 | br71xx | br6511 | cancel-upgrade | load-image | rf-domain]
ap-upgrade[<DEVICE-NAME> | br650 | br71xx | br6511] all {no-reboot/reboot-time
<WORD>/upgrade-time <WORD>}}
ap-upgrade all {no-reboot/reboot-time <WORD>/upgrade-time <WORD>}
ap-upgrade cancel-upgrade [<DEVICE-NAME> | br650 | br71xx | br6511] all
ap-upgrade cancel-upgrade all
ap-upgrade load-image [br650 | br71xx | br6511] <URL>
ap-upgrade rf-domain <DOMAIN-NAME> {no-reboot/no-via-rf-domain/reboot-time
<WORD>/upgrade-time <WORD>}
ap-upgrade rf-domain <DOMAIN-NAME> no-via-rf-domain {no-reboot/reboot-time
<WORD>/upgrade-time <WORD>}

```

#### Parameters

[<DEVICE-NAME> |all |br650  
|br71xx|br6511|  
cancel-upgrade|load-image|  
rf-domain]

- <DEVICE-NAME> all {no-reboot|reboot-time <WORD>|upgrade-time <WORD>} – Specify the name/MAC address of an AP
  - all {no-reboot|reboot-time <WORD>|upgrade-time <WORD>} – Upgrades all the access points
  - br650 all {no-reboot|reboot-time <WORD>|upgrade-time <WORD>} – Upgrades an BR650 device
  - br6511 all {no-reboot|reboot-time <WORD>|upgrade-time <WORD>} – Upgrades a Mobility 6511 Access Point
  - br71xx all {no-reboot|reboot-time <WORD>|upgrade-time <WORD>} – Upgrades a Mobility 7131 Series Access Point
  - cancel-upgrade [<DEVICE-NAME>|br650|br71xx|br6511|all] – Cancels upgrading the AP
  - load-image [br650|br71xx|br6511] <URL> – Loads the AP firmware images on the Controller
    - <URL> – Specify the location of firmware image
      - URLs: tftp://<hostname|IP>[:port]/path/file
      - ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
      - sftp://<user>:<passwd>@<hostname|IP>[:port]/path/file
      - http://<hostname|IP>[:port]/path/file
      - cf:/path/file
      - usb1:/path/file
      - usb2:/path/file
  - rf-domain <DOMAIN-NAME> {no-reboot|no-via-rf-domain|reboot-time <WORD>|upgrade-time <WORD>} – Upgrades all the access points belonging to an RF Domain
    - no-via-rf-domain – Upgrades APs from the adopted device
- The following are common for all the above:
- no-reboot – No reboot (manually reboot after the upgrade)
  - reboot-time <WORD> – Sets the scheduled reboot time
  - upgrade-time <WORD> – Sets the scheduled upgrade time
    - <WORD> – Specify the reboot time in MM/DD/YYYY-HH:MM or HH:MM format

**Example**

```
RFController>ap-upgrade br650 00-A0-F8-00-00-00
RFController>
```

```
RFController>ap-upgrade all
RFController>
```

```
RFController>ap-upgrade default/RFController no-reboot
```

```
-----
CONTROLLER          STATUS          MESSAGE
-----
00-23-68-88-0D-A7   Success        Queued 0 APs to upgrade
-----
```

```
RFController>
```

```
RFController#ap-upgrade RFController reboot-time 06/01/2011-12:10
```

```
-----
CONTROLLER          STATUS          MESSAGE
-----
00-15-70-37-FA-BE   Success        Queued 0 APs to upgrade
-----
```

```
RFController#
```

## change-passwd

### User exec commands

Changes the password of the logged in user

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
change-passwd {<OLD-PASSWD> <NEW-PASSWD>}
```

### Parameters

---

{<OLD-PASSWD> <NEW-PASSWD>}	Optional. The passwords can also be changed interactively. To do so, press Enter after the <b>change-passwd</b> command. <ul style="list-style-type: none"><li>• &lt;OLD-PASSWD&gt; - The password that needs to be changed</li><li>• &lt;NEW-PASSWD&gt; - The password to change to.</li></ul>
--------------------------------	---

---

### Usage Guidelines

A password must be between 8 to 32 characters in length.

### Example

```
RFController>change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
RFController>write memory
OK
RFController>
```



## clear

### *User exec commands*

Clears parameters, cache entries, table entries, and other similar entries. The clear command is only available for specific commands. The information cleared using this command varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

---

### **NOTE**

Refer to the interface details below when using clear:

- ge <index> – Mobility RFS4000 Controller supports 4GEs and the Mobility RFS6000 Controller supports 8 GEs

- me1 – Available in both Mobility RFS7000 Controller and Mobility RFS6000 Controller

---

### **Syntax**

```
clear [arp-cache|cdp|crypto|event-history|ip|lldp|spanning-tree]
clear arp-cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear crypto [ipsec|isakmp] sa [<IP>|all] {on <DEVICE-NAME>}
clear event-history
clear ip dhcp bindings [<A.B.C.D>|all] {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface {<INTERFACE>|ge
<1-8>|me1|port-channel <1-4>|vlan <1-4094>} {on <DEVICE-NAME>}}
```

#### Parameters

arp-cache {on <DEVICE-NAME>}	<p>Clears ARP cache entries.</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the arp cache on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul>
[cdp lldp] neighbors {on <DEVICE-NAME>}	<p>Clears Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) neighbor table entries</p> <ul style="list-style-type: none"> <li>neighbors – Clears CDP neighbor table <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul> </li> </ul>
crypto [ipsec isakmp] sa [<IP> all] {on <DEVICE-NAME>}	<p>Clears the encryption module's databases.</p> <ul style="list-style-type: none"> <li>ipsec sa – Clears IPSEC security associations.</li> <li>isakmp sa – Clears ISAKMP security associations.</li> </ul> <p>The following are common for the above:</p> <ul style="list-style-type: none"> <li>&lt;IP&gt; – Clears the IPSec or ISAKMP security associations for a certain Peer.</li> <li>all – Clears the IPSec or ISAKMP security associations for all Peers. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the SAs on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul> </li> </ul>
event-history	Clears event history
ip dhcp bindings [<IP> all] {on <DEVICE-NAME>}	<p>Clears the DHCP address bindings.</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul>
spanning-tree detected-protocols {interface <INTERFACE> ge <1-8> me1 port-channel <1-4> vlan <1-4094>} {on <DEVICE-NAME>}	<p>Clears the spanning-tree protocols configured for the interface</p> <ul style="list-style-type: none"> <li>detected-protocols {interface [&lt;INTERFACE&gt; ge &lt;1-8&gt; me1 port-channel &lt;1-4&gt; vlan &lt;1-4094&gt;]} {on} – Enter the interface name to clear the detected spanning tree protocols for that specific interface <ul style="list-style-type: none"> <li>&lt;INTERFACE&gt; – Clears selected interface name</li> <li>ge &lt;1-8&gt; – Clears the configured GigabitEthernet interface status</li> <li>me1 – Clears the FastEthernet interface status</li> <li>port-channel &lt;1-4&gt; – Clears port-channel information on AP/Controller</li> <li>vlan &lt;1-4094&gt; – Clears the configured vlan information</li> <li>wwan1 – Clears Wireless WAN interface information</li> </ul> </li> </ul> <p>The following are common for the above</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul>

#### Example

```
RFController>clear crypto isakmp sa 111.222.333.01 on RFController
RFController>
```

```
RFController>clear event-history
RFController>
```

```
RFController>clear spanning-tree detected-protocols interface port-channel 1
on RFController
RFController>
```

```
RFController>clear ip dhcp bindings 172.16.10.9 on RFController  
RFController>
```

```
RFController#clear cdp neighbors on RFController  
RFController#  
RFController#clear spanning-tree detected-protocols interface ge 1  
RFController#
```

```
RFController#clear lldp neighbors  
RFController#
```

## clock

### *User exec commands*

Configures the system clock

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

### Parameters

---

set <HH:MM:SS> <1-31> <MONTH>  
<1993-2035> {on <DEVICE-NAME>}

- Sets the software system clock for the configured device
    - <HH:MM:SS> – Sets the current time (in military format hours, minutes and seconds)
    - <1-31> – Enter the numerical day of the month
      - <MONTH> – Enter the month of the year (Jan to Dec)
      - <1993-2035> – Select a valid digit year from 1993-2035
      - on – On AP/Controller
      - <DEVICE-NAME> – On AP/Controller name
- 

### Example

```
RFController>clock set 12:30:45 2 MONTH 2010 on RFController  
clock set 12:30:45 2 MONTH 2010 on RFController RFController>
```

## cluster

### *User exec commands*

Use this command to initiate the cluster context. The cluster context provides centralized management to configure all the cluster members from any one member.

Commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
cluster start-selection
```

### Parameters

---

start-selection	Starts a new cluster master election
-----------------	--------------------------------------

---

### Example

```
RFController>cluster start-election  
RFController>
```

### commit

#### *User exec commands*

Commits all the changes made in the active session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
commit {write memory}
```

#### **Parameters**

---

write memory	If a commit succeeds, the configuration is written to memory
	<ul style="list-style-type: none"><li>• memory - Writes the changes to memory</li></ul>

---

#### **Example**

```
RFController>commit write memory  
[OK]  
RFController>
```

## connect

### *User exec commands*

Begins a console connection to a remote device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
connect [mint-id MINT-ID|REMOTE-DEVICE-NAME]
```

### Parameters

mint-id <MINT-ID>	Connects to the remote system using MINT ID. <ul style="list-style-type: none"> <li>• &lt;MINT-ID&gt; - The MINT Id of the remote device.</li> </ul>
<REMOTE-DEVICE-NAME>	Connects to the remote system using its device name.

### Example

```
RFController>connect RFDOMAIN UseCase1/RFController

Entering character mode
Escape character is '^]'.
RFS7000 release 5.1.0.0
RFController login: admin
Password:
Welcome to CLI
RFController>
```

## crypto

### User exec commands

Enables encryption

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
crypto [key|pki]

crypto key [export|generate|import|zeroise]
crypto key export rsa <RSA-KEYPAIR-NAME>> <EXPORT-TO-URL>
    {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
    {background} {on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase
<KEY-PASSPHRASE>} {background} {on <DEVICE-NAME>}

crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048>
    {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
    {background} {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> passphrase
<KEY-PASSPHRASE> {background} {on <DEVICE-NAME>}

crypto key zeroise rsa <RSA-KEYPAIR-NAME> {force} {on <DEVICE-NAME>}

crypto pki [authenticate|export|generate|import|zeroise]
crypto pki authenticate <TRUST-POINT> <URL> {background} {on <DEVICE-NAME>}

crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|use-rsa-key]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
[autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name (<EXPORT-TO-URL>,email <SEND-TO-EMAIL>,fqdn
<FQDN>,ip-address <IP>)

crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name <EXPORT-TO-URL> {background} {on <DEVICE-NAME>}

crypto pki export request [generate-rsa-key|use-rsa-key] <WORD> subject-name
<COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANISATION> <ORGANIZATION-UNIT>
[<EXPORT-TO-URL>|email <SEND-TO-EMAIL>|fqdn <FQDN>|ip-address <IP>]
```



```
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {{background}
{on <DEVICE--NAME>}/passphrase <KEY-PHRASE> {background} {on <DEVICE-NAME>}/on
<DEVICE-NAME>}}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> [autogen-subject-name|subject-name]
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name
{email/fqdn/ip-address/on}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name email <WORD> {fqdn
<WORD>/ip-address <A.B.C.D>/on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name fqdn <WORD> {email
<WORD>/ip-address <A.B.C.D>/on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name ip-address
<A.B.C.D> {fqdn <WORD>/on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name {on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> subject-name <COMMON-NAME> <COUNTRY>
<STATE> <CITY> <ORGANISATION> <ORGANIZATION-UNIT> {email <WORD>/fqdn
<WORD>/ip-address <A.B.C.D>/on} <DEVICE-NAME>
```

```
crypto pki import [certificate|crl|trustpoint]
```

```
crypto pki import [certificate|crl] <WORD> <IMPORT-FROM-URL> {background {on
<DEVICE-NAME>}/on <DEVICE--NAME>}}
```

```
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background
{on <DEVICE-NAME>}/on <DEVICE-NAME>/passphrase <word> {background {on
<DEVICE-NAME>}/on <DEVICE-OR-DOMAIN-NAME>}
```

```
crypto pki zeroise trustpoint <TRUSTPOINT-NAME> {del-key {on
<DEVICE-OR-DOMAIN-NAME>}/on <DEVICE-NAME>}
```

#### Parameters

key	Performs key management operations
key export	<ul style="list-style-type: none"> <li>• export rsa &lt;RSA-KEYPAIR-NAME&gt; &lt;EXPORT-TO-URL&gt; {background   on   phrase} – Performs export operation</li> <li>• rsa &lt;RSA-KEYPAIR-NAME&gt; – Enter the name of a RSA keypair to export               <ul style="list-style-type: none"> <li>• &lt;EXPORT-TO-URL&gt; {background   on   phrase} – Enter the location to send the key using the following syntax:                    tftp://&lt;hostname   IP&gt;[:port]/path/file                    ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname   IP&gt;[:port]/path/file                    sftp://&lt;user&gt;@&lt;hostname   IP&gt;[:port]/path/file                    http://&lt;hostname   IP&gt;[:port]/path/file                    cf:/path/file                    usb1:/path/file                    usb2:/path/file                 </li> <li>• background {on &lt;DEVICE-NAME&gt;} – Performs the operation in background</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> <li>• passphrase &lt;KEY-PASSPHRASE&gt; {background   on } – Enter a passphrase to encrypt the RSA key (aes-128)</li> <li>• background {on &lt;DEVICE-NAME&gt;} – Performs the operation in the background</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> </li> </ul>
key generate	<ul style="list-style-type: none"> <li>• generate rsa &lt;RSA-KEYPAIR-NAME&gt; &lt;1024-2048&gt; {on &lt;DEVICE-NAME&gt;} – Generates a keypair               <ul style="list-style-type: none"> <li>• rsa &lt;WORD&gt; – Enter the name of a RSA keypair to generate                   <ul style="list-style-type: none"> <li>• &lt;1024-2048&gt; – Enter the size of the RSA key in bits from 1024-2048</li> <li>• on &lt;DEVICE-NAME&gt; – On an AP or a Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> </li> </ul> </li> </ul>

key import	<ul style="list-style-type: none"> <li>• import rsa &lt;RSA-KEYPAIR-NAME&gt; &lt;IMPORT-FROM-URL&gt; {background {on &lt;DEVICE-NAME&gt;}} on &lt;DEVICE-NAME&gt;} passphrase} - Performs an import operation           <ul style="list-style-type: none"> <li>• rsa &lt;RSA-KEYPAIR-NAME&gt; - Enter the name of a RSA keypair to import               <ul style="list-style-type: none"> <li>• &lt;IMPORT-FROM-URL&gt; {background on phrase} - Enter the location to send the key using the following formats:                    tftp://&lt;hostname IP&gt;[:port]/path/file                    ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file                    sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file                    http://&lt;hostname IP&gt;[:port]/path/file                    cf:/path/file                    usb1:/path/file                    usb2:/path/file                 </li> <li>• background {on &lt;DEVICE-NAME&gt;} - Performs the operation in the background</li> <li>• on &lt;DEVICE-NAME&gt; - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> <li>• on &lt;DEVICE-NAME&gt;} - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> <li>• passphrase &lt;KEY-PASSPHRASE&gt;&gt; {background on} - Enter a passphrase to decrypt the RSA key (aes-128)</li> <li>• background {on &lt;DEVICE-NAME&gt;} - Performs the operation in background</li> <li>• on &lt;DEVICE-NAME&gt; - On an AP or a Controller</li> </ul> </li> </ul> </li> </ul>
key zeroize	<ul style="list-style-type: none"> <li>• zeroize rsa &lt;RSA-KEYPAIR-NAME&gt; {force {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}} on &lt;DEVICE-NAME&gt;} - Performs delete operation           <ul style="list-style-type: none"> <li>• rsa &lt;RSA-KEYPAIR-NAME&gt; - Deletes the specified RSA key               <ul style="list-style-type: none"> <li>• force {on &lt;DEVICE-NAME&gt;} - Forces the deletion of all certificates associated with the key                   <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> <li>• on &lt;DEVICE-NAME&gt;} - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> </ul> </li> </ul> </li> </ul> </li> </ul>
pki [authenticate export generate import zeroize]	Performs PKI related commands
pki authenticate <trustpoint-name> <URL> {background} {on <DEVICE-name>}	<ul style="list-style-type: none"> <li>• authenticate &lt;TRUSTPOINT-NAME&gt; - Authenticates and imports ca certificate           <ul style="list-style-type: none"> <li>• &lt;URL&gt; (background on) - Enter the location of ca certificate to authenticate                tftp://&lt;hostname IP&gt;[:port]/path/file                ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file                sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file                http://&lt;hostname IP&gt;[:port]/path/file                cf:/path/file                usb1:/path/file                usb2:/path/file             </li> <li>• {background} {on &lt;DEVICE-NAME&gt;} - Performs the operation in the background               <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> <li>• on &lt;DEVICE-NAME&gt;} - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> </ul> </li> </ul> </li> </ul>

- 
- crypto pki export request  
 [generate-rsa-key | use-rsa-key]  
 <RSA-KEYPAIR-NAME>  
 [autogen-subject-name | subject-name]
- export – Performs export operation
    - request [generate-rsa-key | use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] [<EXPORT-TO-URL> | email | fqdn | ip-address] – Generates and exports a Certificate Signing Request
      - generate-rsa-key <RSA-KEYPAIR-NAME> – Generates a new RSA key-pair
      - use-rsa-key – Uses a generated RSA key-pair
- The following parameters are common for the above:
- RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] – Enter the name of RSA key-pair to export
  - autogen-subject-name – Autogenerates the subject name from config parameters
  - URL – Enter the URL to export the CSR
    - fttp://<hostname | IP>[:port]/path/file
    - ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file
    - sftp://<user>@<hostname | IP>[:port]/path/file
    - http://<hostname | IP>[:port]/path/file
    - cf:/path/file
    - usb1:/path/file
    - usb2:/path/file
  - email – Enter the email address
  - fqdn – Enter the fully qualified domain name
  - ip-address – Enter the IP Address
- 
- subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> {email <EMAIL> | fqdn <FQDN> | ip-address <IP> | on <DEVICE-OR-DOMAIN-NAME>} – Enter the subject name to identify the certificate
  - <COMMON-NAME> – Enter the common name used with the ca certificate
  - <COUNTRY> – Enter the deployment country (2 character ISO code)
  - <STATE> – Enter the state (2 to 64 characters)
  - <CITY> – Enter the city (2 to 64 characters)
  - <ORGANIZATION> – Enter the organization name (2 to 64 characters)
  - <ORGANIZATION-UNIT> – Enter the organization unit name (2 to 64 characters)
  - email <WORD> – Enter the email address
  - fqdn – Enter the fully qualified domain name
  - ip-address <A.B.C.D> – Enter the IP Address
  - on <DEVICE-NAME> – On AP/Controller
  - <DEVICE-NAME> – AP/Controller name

---

<pre>export trustpoint &lt;TRUSTPOINT-NAME&gt; &lt;EXPORT-TO-URL&gt; {background} {on &lt;DEVICE-NAME&gt;}</pre>	<p>Exports a trustpoint (CA cert, CRL, server cert and private key).</p> <ul style="list-style-type: none"><li>• &lt;TRUSTPOINT-NAME&gt; – Enter the trust point name</li><li>• &lt;EXPORT-TO-URL&gt; (background on) – Enter the location of ca certificate to import</li></ul> <p>URLs: tftp://&lt;hostname IP&gt;[:port]/path/file ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file http://&lt;hostname IP&gt;[:port]/path/file cf:/path/file usb1:/path/file usb2:/path/file</p> <ul style="list-style-type: none"><li>• background {on &lt;DEVICE-NAME&gt;} – Performs the operation in background</li><li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li><li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li><li>• on &lt;DEVICE-NAME&gt;} – On AP/Controller</li><li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li></ul>
--	---

- 
- generate self-signed  
 <TRUSTPOINT-NAME>  
 [generate-rsa-key | use-rsa-key]  
 <RSA-KEYPAIR-NAME>
- generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key | use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] - Generates Operation
    - self-assigned - Generates a self-signed certificate (and trustpoint with it)
      - <TRUSTPOINT-NAME> [generate-rsa-key | use-rsa-key] - Enter the trust point name
        - generate-rsa-key - Generates a new RSA key-pair
        - use-rsa-key - Uses a generated RSA key-pair
- The following parameters are common for the above:
- <RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] - Enter the name of RSA key-pair to export
  - autogen-subject-name - Autogenerates the subject name from config parameters
  - URL - Enter the URL to export the CSR to  
 URLs: tftp://<hostname | IP>[:port]/path/file  
 ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file  
 sftp://<user>@<hostname | IP>[:port]/path/file  
 http://<hostname | IP>[:port]/path/file  
 cf:/path/file  
 usb1:/path/file  
 usb2:/path/file
  - email - Enter a destination email address
  - fqdn - Enter the fully qualified domain name
  - ip-address - Enter an IP Address
  - subject-name <Common-Name> <Country> <State> <City> <Organization> <Organization-Unit> {email<WORD> | fqdn <WORD> | ip-address <A.B.C.D> | on} <DEVICE-OR-DOMAIN-NAME> - Enter the subject name to identify the certificate
  - <Common-Name> - Enter the common name used with the certificate
  - <Country> - Enter the country (2 character ISO code)
  - State - Enter the state (2 to 64 characters)
  - City - Enter the city (2 to 64 characters)
  - <Organization> - Enter the Organization name (2 to 64 characters)
  - <Organization-Unit> {email <WORD> | fqdn <WORD> | ip-address <A.B.C.D> | on} - Enter the Organization unit name (2 to 64 characters)
  - email <WORD> - Enter the email address
  - fqdn - Enter the fully qualified domain name
  - ip-address <A.B.C.D> - Enter the IP Address
  - on <DEVICE-NAME > - On AP/Controller
  - <DEVICE-NAME> - AP/Controller name

---

<pre>import [certificate   crl   trustpoint]</pre>	<p>Imports certificates, certificate revocation list or a trustpoint to the selected device.</p> <ul style="list-style-type: none"> <li>• <code>certificate &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt; {background} {on &lt;DEVICE-NAME&gt;} on &lt;DEVICE-NAME&gt;</code> – Imports the signed server certificate       <ul style="list-style-type: none"> <li>• <code>&lt;TRUSTPOINT-NAME&gt;</code> – Enter the name of the trustpoint (should be already authenticated)           <ul style="list-style-type: none"> <li>• <code>&lt;IMPORT-FROM-URL&gt;</code> – Enter the URL to import from                URLs: <code>ftp://&lt;hostname IP&gt;[:port]/path/file</code>  <code>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</code>  <code>sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file</code>  <code>http://&lt;hostname IP&gt;[:port]/path/file</code>  <code>cf:/path/file</code>  <code>usb1:/path/file</code>  <code>usb2:/path/file</code></li> </ul> </li> </ul> </li> <li>• <code>crl &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt; {background} {on &lt;DEVICE-NAME&gt;} on &lt;DEVICE-NAME&gt;</code> – Imports a Certificate revocation list       <ul style="list-style-type: none"> <li>• <code>&lt;TRUSTPOINT-NAME&gt;</code> – Enter the name of trustpoint to which CRL belongs           <ul style="list-style-type: none"> <li>• <code>&lt;IMPORT-FROM-URL&gt;</code> – URL to import CRL from                URLs: <code>ftp://&lt;hostname IP&gt;[:port]/path/file</code>  <code>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname IP&gt;[:port]/path/file</code>  <code>sftp://&lt;user&gt;@&lt;hostname IP&gt;[:port]/path/file</code>  <code>http://&lt;hostname IP&gt;[:port]/path/file</code>  <code>cf:/path/file</code>  <code>usb1:/path/file</code>  <code>usb2:/path/file</code></li> </ul> </li> </ul> </li> </ul> <p>The following parameters are common for certificate and crl:</p> <ul style="list-style-type: none"> <li>• <code>background {on &lt;DEVICE-NAME&gt;}</code> – Performs the operation in background</li> <li>• <code>on &lt;DEVICE-NAME&gt;</code> – On AP/Controller</li> <li>• <code>&lt;DEVICE-NAME&gt;</code> – On AP/Controller name</li> <li>• <code>on &lt;DEVICE-NAME&gt;}</code> – On AP/Controller</li> <li>• <code>&lt;DEVICE-NAME&gt;</code> – On AP/Controller name</li> </ul>
--	---

- 
- `trustpoint <WORD> URL {background {on <DEVICE-OR-DOMAIN-NAME>} | on <DEVICE-NAME> | passphrase <word> {background {on <DEVICE-NAME>} | on <DEVICE-NAME>}} - Imports a trustpoint, includes CA certificate, server certificate and private key`
  - `<WORD>` - Enter the name of the trustpoint name
    - `URL (background | on)` - Enter the location to import trustpoint from
- URLs: `tftp://<hostname>|IP>[:port]/path/file`  
`ftp://<user>:<passwd>@<hostname>|IP>[:port]/path/file`  
`sftp://<user>@<hostname>|IP>[:port]/path/file`  
`http://<hostname>|IP>[:port]/path/file`  
`cf:/path/file`  
`usb1:/path/file usb2:/path/file`
  - `background {on <DEVICE-NAME>}` - Performs the operation in background
  - `on <DEVICE-NAME>` - On AP/Controller
  - `<DEVICE-NAME>` - On AP/Controller name
  - `on <DEVICE-NAME>` - On AP/Controller
  - `<DEVICE-OR-DOMAIN-NAME>` - On AP/Controller name
  - `passphrase <WORD> {background | on}` - Enter a passphrase if the private key is to be exported encrypted
  - `background {on <DEVICE-NAME>}` - Performs the operation in background
  - `zeroise trustpoint <TRUSTPOINT-NAME> {del-key} {on <DEVICE-NAME>}` - Performs delete operation
  - `trustpoint <WORD>` - Enter the name of the trustpoint to delete
    - `del-key {on <DEVICE-NAME>}` - Deletes the private key associated to the server certificate
      - `on <DEVICE-NAME>` - On AP/Controller
      - `<DEVICE-NAME>` - On AP/Controller name

---



**Example**

```
RFController>crypto key generate rsa key 1025
RSA Keypair successfully generated
RFController>
```

```
RFController>crypto key import rsa admin123 url passphrase word background on
RFController
RSA key import operation is started in background
RFController>
```

```
RFController>crypto pki generate self-signed word generate-rsa-key word
autogen-subject-name fqdn word
Successfully generated self-signed certificate
RFController>
```

```
RFController#crypto pki zeroize trustpoint word del-key on RFController
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using
default-trustpoint
RFController#
```

```
RFController>crypto pki authenticate word url background on RFController
Import of CA certificate started in background
RFController>
```

```
RFController>crypto pki import trustpoint word url passphrase word on
RFController
Import operaton started in background
RFController>
```

### disable

#### *User exec commands*

Turns off (disables) the privileged mode command set. This command is not applicable in the Privileged Executable mode.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
disable
```

#### **Parameters**

None

#### **Example**

```
RFController>disable  
RFController>
```

## enable

### *User exec commands*

Turns on (enables) the privileged mode command set. This command is not applicable in the Privileged Executable mode.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
enable
```

### **Parameters**

None

### **Example**

```
RFController>enable  
RFController#
```

### exit

#### *User exec commands*

Ends the current CLI session and closes the session window.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
exit
```

#### **Parameters**

None

#### **Example**

```
RFController>exit
```

## help

### *User exec commands*

Describes the interactive help system.

Use this command to access the advanced help feature. Use “?” anytime at the command prompt to access the help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
help {show configuration-tree/search}
help search <WORD> {detailed/only-show/skip-show}
```

### Parameters

show configuration-tree	Displays running system information <ul style="list-style-type: none"> <li>• configuration-tree – Displays the relationships among configuration objects</li> </ul>
search <WORD> {detailed only-show skip-show}	Searches for CLI commands related to a specific term <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter a term to search CLI commands for (Eg: a feature or a configuration parameter)               <ul style="list-style-type: none"> <li>• detailed – Searches and displays help strings in addition to mode and commands</li> <li>• only-show – Displays only "show" commands, not the configuration commands</li> <li>• skip-show – Displays only configuration commands, not "show" commands</li> </ul> </li> </ul>

### 3 User exec commands

#### Example

```
RFController>help search crypto detailed
Found 29 references for "crypto"

Mode      : User Exec
Command   : show crypto key rsa (|public-key-detail) (|(on
DEVICE-OR-DOMAIN-NAME))
          \ Show running system information
          \ Encryption related commands
          \ Key management operations
          \ Show RSA public Keys
          \ Show the public key in PEM format
          \ On AP/Controller or RF-Domain
          \ AP / Controller / RF-Domain name

: show crypto pki trustpoints (WORD|all|)(|(on DEVICE-OR-DOMAIN-NAME))
  \ Show running system information
  \ Encryption related commands
  \ Public Key Infrastructure related commands
  \ Display the configured trustpoints
  \ Display a particular trustpoint's details
  \ Display details for all trustpoints
  \ On AP/Controller or RF-Domain
  \ AP / Controller / RF-Domain name

: show crypto isakmp sa (|(on DEVICE-NAME))
  \ Show running system information
  \ Encryption Module
  \ Show ISAKMP related statistics
  \ Show all ISAKMP Security Associations
  \ On AP/Controller
  \ AP / Controller name

: show crypto ipsec sa (|(on DEVICE-NAME))
  \ Show running system information
  \ Encryption Module
  \ Show IPSec related statistics
  \ IPSec security association
  \ On AP/Controller
  \ AP / Controller name

: clear crypto isakmp sa (A.B.C.D|all) (|(on DEVICE-NAME))
  \ Clear
  \ Encryption Module
  \ ISAKMP database
  \ Flush ISAKMP SAs
  \ Fluch ISAKMP SAs for a given peer
.....
.....RFCont
roller>
```

```
RFController>help show configuration-tree
```

```
## ACCESS-POINT / Controller ## ---+
|
+--> [[ RF-DOMAIN ]]
|
+--> [[ PROFILE ]]
|
```

```

                                +--> Device specific parameters (license, serial
number, hostname)
                                |
                                +--> Configuration Overrides of rf-domain and
profile

## RF-DOMAIN ## ---+
|
+--> RF parameters, WIPS server parameters
|
+--> [[ SMART-RF-POLICY ]]
|
+--> [[ WIPS POLICY ]]

## PROFILE ## ---+
|
+--> Physical interface (interface GE,ME,UP etc)
|
|                                     +--> [[ RATE-LIMIT-TRUST-POLICY ]]
|
+--> Vlan interface (interface VLAN1/VLAN36 etc)
|
+--> Radio interface (interface RADIO1, RADIO2 etc)
|
|                                     +--> Radio specific Configuration
|                                     |
|                                     +--> [[ RADIO-QOS-POLICY ]]
|                                     |
|                                     +--> [[ ASSOC-ACL-POLICY ]]
|                                     |
|                                     +--> [[ WLAN ]]
|
+--> [[ MANAGEMENT-POLICY ]]
|
+--> [[ DHCP-SERVER-POLICY ]]
|
+--> [[ FIREWALL-POLICY ]]
|
+--> [[ NAT-POLICY ]]

.....
.....RFCont
roller>

RFController>help search clrscr only-show
found no commands containing "clrscr"
RFController>

RFController>help search service skip-show
Found 32 references for "service"

Mode      : User Exec
Command   : service show cli
           : service show rim config (|include-factory)
           : service show wireless credential-cache
           : service show wireless neighbors
           : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
           : service show process(|(on DEVICE-OR-DOMAIN-NAME))
           : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
           : service show top(|(on DEVICE-OR-DOMAIN-NAME))

```

### 3 User exec commands

```
      : service show crash-info ( |(on DEVICE-OR-DOMAIN-NAME))
      : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
      : service cli-tables-expand (|left|right)
      : service wireless clear unauthorized aps ( |(on DEVICE-OR-DOMAIN-NAME))
      : service wireless qos delete-tspeg AA-BB-CC-DD-EE-FF tid <0-7>
      : service wireless wips clear-event-history
      : service wireless wips clear-mu-blacklist (all|(mac
AA-BB-CC-DD-EE-FF))
      : service radio <1-3> dfs simulate-radar (primary|extension)
      : service smart-rf run-calibration
      : service smart-rf stop-calibration
      : service cluster manual-revert
      : service advanced-wips clear-event-history
      : service advanced-wips clear-event-history
(dos-eap-failure-spoof|id-theft-out-of-sequence|id-theft-eapol-success-spoof-
detected|wlan-jack-attack-detected|ssid-jack-attack-detected|monkey-jack-att
ack-detected|null-probe-response-detected|fata-jack-detected|fake-dhcp-server
-detected|crackable-wep-iv-used|windows-zero-config-memory-leak|multicast-all
-systems-on-subnet|multicast-all-routers-on-subnet|multicast-ospf-all-routers
-detection|multicast-ospf-designated-routers-detection|multicast-rip2-routers
-detection|multicast-igmp-routers-detection|multicast-vrrp-agent|multicast-hs
rp-agent|multicast-dhcp-server-relay-agent|multicast-igmp-detection|netbios-d
etection|stp-detection|ipx-detection|invalid-management-frame|invalid-channel
-advertized|dos-deauthentication-detection|dos-disassociation-detection|dos-r
ts-flood|rogue-ap-detection|accidental-association|probe-response-flood|dos-c
ts-flood|dos-eapol-logoff-storm|unauthorized-bridge)
      : service start-shell
      : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio
(all|<1-3>) (|promiscuous)|rim|interface `WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>')(|{direction (any|inbound|outbound)|acl-name WORD|verbose|hex|count
<1-1000000>|snap <1-2048>|write (FILE|URL|tzsp WORD)|tcpdump}) (|filter LINE)

Mode      : Profile Mode
Command   : service watchdog

Mode      : Radio Mode
Command   : service antenna-type
(default|dual-band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|br
650-int)
      : service disable-erp
      : service disable-ht-protection
      : service recalibration-interval <0-65535>
.....RFC
ontroller>

RFCController>help search mint only-show
Found 8 references for "mint"

Mode      : User Exec
Command   : show mint neighbors (|details)(|(on DEVICE-NAME))
      : show mint links (|details)(|(on DEVICE-NAME))
      : show mint id(|(on DEVICE-NAME))
      : show mint stats(|(on DEVICE-NAME))
      : show mint route(|(on DEVICE-NAME))
      : show mint lsp
      : show mint lsp-db (|details)(|(on DEVICE-NAME))
      : show mint mlcp(|(on DEVICE-NAME))
RFCController>
```



## logging

### *User exec commands*

Modifies message logging facilities

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
logging [monitor] {<0-7>|alerts|critical|debugging|
emergencies|errors|informational|notifications|warnings}
```

### Parameters

---

[monitor]	• monitor – Sets the terminal lines logging level
{<0-7> alerts critical debugging	• <0-7> – Enter the logging severity level from 0-7
g	• alerts – Immediate action needed (severity=1)
emergencies errors	• critical – Critical conditions (severity=2)
informational notifications war	• debugging – Debugging messages (severity=7)
nings}	• emergencies – System is unusable (severity=0)
	• errors – Error conditions (severity=3)
	• informational – Informational messages (severity=6)
	• notifications – Normal but significant conditions (severity=5)
	• warnings – Warning conditions (severity=4)

---

### Example

```
RFController>logging monitor warnings ?
RFController>

RFController>logging monitor 2
RFController>
```

## mint

### User exec commands

Configures MiNT protocol

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mint [ping|traceroute]
mint ping MINT-ID {count <1-60>|size <1-64000>|timeout <1-10>}
mint traceroute MINT-ID {destination-port <1-65535>|max-hops <1-255>|
source-port <1-65535>|timeout <1-255>}
```

### Parameters

ping MINT-ID {count <1-60> size <1-64000> timeout <1-10>}	<p>Sends a MiNT echo message to a MiNT destination</p> <ul style="list-style-type: none"> <li>• MINT-ID – Enter the MiNT destination id to ping <ul style="list-style-type: none"> <li>• count &lt;1-60&gt; – Enter the number of times to ping from 1-60. The default value is 3</li> <li>• size &lt;1-64000&gt; – Enter the size of the MiNT payload in bytes from 1-64000. The default value is 64</li> <li>• timeout &lt;1-10&gt; – Enter the time for a response after sending a ping request from 1-10 seconds. The default timeout is 1 second</li> </ul> </li> </ul>
traceroute MINT-ID {destination-port <1-65535> max-hops <1-255> source-port <1-65535> timeout <1-255>}	<p>Print the route packets trace to a device</p> <ul style="list-style-type: none"> <li>• MINT-ID – Enter the MiNT destination id <ul style="list-style-type: none"> <li>• destination-port &lt;1-65535&gt; – Enter the destination port value to be used for ECMP (default 45)</li> <li>• max-hops &lt;1-255&gt; – Enter the maximum number of hops, a traceroute packet traverses in forward direction.(default 30)</li> <li>• source-port &lt;1-65535&gt; – Enter the source port value to be used for ECMP (default 45)</li> <li>• timeout &lt;1-65535&gt; – Enter the time to wait for a response (default 30 seconds)</li> </ul> </li> </ul>

### Example

```
RFController>mint ping 70.37.FA.BF count 20 size 128
MiNT ping 70.37.FA.BF with 128 bytes of data.
Response from 70.37.FA.BF: id=1 time=0.292 ms
Response from 70.37.FA.BF: id=2 time=0.206 ms
Response from 70.37.FA.BF: id=3 time=0.184 ms
Response from 70.37.FA.BF: id=4 time=0.160 ms
Response from 70.37.FA.BF: id=5 time=0.138 ms
Response from 70.37.FA.BF: id=6 time=0.161 ms
Response from 70.37.FA.BF: id=7 time=0.174 ms
Response from 70.37.FA.BF: id=8 time=0.207 ms
```

```
Response from 70.37.FA.BF: id=9 time=0.157 ms
Response from 70.37.FA.BF: id=10 time=0.153 ms
Response from 70.37.FA.BF: id=11 time=0.159 ms
Response from 70.37.FA.BF: id=12 time=0.173 ms
Response from 70.37.FA.BF: id=13 time=0.156 ms
Response from 70.37.FA.BF: id=14 time=0.209 ms
Response from 70.37.FA.BF: id=15 time=0.147 ms
Response from 70.37.FA.BF: id=16 time=0.203 ms
Response from 70.37.FA.BF: id=17 time=0.148 ms
Response from 70.37.FA.BF: id=18 time=0.169 ms
Response from 70.37.FA.BF: id=19 time=0.164 ms
Response from 70.37.FA.BF: id=20 time=0.177 ms
```

```
--- 70.37.FA.BF ping statistics ---
```

```
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.177/0.292 ms
```

### no

#### *User exec commands*

Use the no command to revert a command or to set parameters to their default values. This command is useful if you would like to turn off an enabled feature or set default values for a parameter.

---

**NOTE**

The commands have their own set of parameters that can be reset.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [adoption|captive-portal|crypto|debug|logging|page|service|
terminal|wireless]
```

**Parameters**

None

**Usage Guidelines**

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

**Example**

```
RFController>no adoption
RFController>

RFController>no page
RFController>

RFController>no service cli-tables-expand line
RFController>
```

## page

### *User exec commands*

Use the command to toggle the Controller paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
page
```

### **Parameters**

None

### **Example**

```
RFController>page  
RFController>
```

### ping

#### *User exec commands*

Sends ICMP echo messages to a user-specified location

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
ping { [<IP>|<hostname> ] }
```

#### **Parameters**

---

ping { [<IP> <hostname> ] }	Pings the specified destination IP address or hostname. When entered without any parameters, this command prompts for an IP/Host-name to ping.
-----------------------------	--

---

#### **Example**

```
RFController>ping 172.16.10.3
PING 172.16.10.3 (172.16.10.3): 100 data bytes
108 bytes from 172.16.10.3: seq=0 ttl=64 time=7.100 ms
108 bytes from 172.16.10.3: seq=1 ttl=64 time=0.390 ms
108 bytes from 172.16.10.3: seq=2 ttl=64 time=0.422 ms
108 bytes from 172.16.10.3: seq=3 ttl=64 time=0.400 ms

--- 172.16.10.3 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.390/2.078/7.100 ms
RFController>
```

## revert

### *User exec commands*

Reverts the changes made in the active session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
revert
```

### **Parameters**

None

### **Example**

```
RFController>revert  
RFController>
```

## service

### User exec commands

The service command performs different functions depending on the parameter passed to it. Generally, this command is used to directly interact with the device to force an action to be performed

---

#### NOTE

Service commands have their own set of parameters that can be used. Please refer to the [Chapter 6, service](#) for a list of parameters used with this command.

---

#### Syntax

```
service
[advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster|force-send-con
fig|locator|noc|radio|radius|set|show|smart-rf|wireless|pktcap]
```

#### Parameters

---

#### NOTE

Please see [Chapter 6, service](#) for more information on the parameters.

---

#### Example

```
RFController>service locator
RFController>service set validation-mode full
RFController>RFController>service show sysinfo
System Information:

Free RAM: 65.2% (166672 of 255464) Min: 10.0%
File Descriptors: free: 24070 used: 1088 max: 25500
CPU load averages: 1 min: 0.5% 5 min: 0.5% 15 min: 0.4%

Kernel Buffers:
Size:      32    64   128   256   512   1k    2k    4k    8k   16k   32k   64k
128k
Usage:    2592  2983   858   162   296   112   136    25   71    1    1    2
0
Limit:   32768  8192  4096  4096  8192  8192 16384 16384 1024  512  256  64
64
RFController>
```



## show

### User exec commands

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances
- When invoked with the display\_parameter, it displays information about that component.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show <parameter>
```

### Parameters

---

### NOTE

Refer to [Chapter 7, Show Commands](#) for more information.

---

### Example

```
RFController>show ?
  adoption                Display information related to adoption to wireless
                           controller
  advanced-wips           Advanced WIPS
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization   Device Categorization
  event-history           Display event history
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  licenses                Show installed licenses and usage
  mac-address-table       Display MAC address table
  mint                   MiNT protocol
  noc                     Noc-level information
```

### 3 User exec commands

ntp	Network time protocol
password-encryption	Pasword encryption
power	Show power over ethernet command
remote-debug	Show details of remote debug sessions
rf-domain-manager	Show RF Domain Manager selection details
role	Role based firewall
running-config	Current operating configuration
session-changes	Configuration changes made in this session
session-config	This session configuration
sessions	Display CLI sessions
smart-rf	Smart-RF Management Commands
spanning-tree	Display spanning tree information
startup-config	Startup configuration
terminal	Display terminal configuration parameters
timezone	The timezone
version	Display software & hardware version
wireless	Wireless commands

RFController>

## telnet

### *User exec commands*

Opens a telnet session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
telnet <IP> {port}
```

### Parameters

---

<IP> {port}	Defines an IP address or hostname of a remote system
	<ul style="list-style-type: none"><li>• port – Enter the TCP port number</li></ul>

---

### Example

```
RFController>telnet 172.16.10.1

Entering character mode
Escape character is '^]'.
RFS7000 release 5.1.0.0
RFController login: cli
NOTE: logging in as 'cli' w/o password is going away. Use admin accounts under
management-policy [Eg: admin/admin123]
Welcome to CLI
RFController>
```

## terminal

### *User exec commands*

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
terminal [length|width] <0-512>
```

### **Parameters**

length <0-512>	Sets the number of lines on a screen
width <0-512>	Sets the width/number of characters on the screen line

### **Example**

```
RFController>terminal length 150
RFController>

RFController>terminal width 215
RFController>
```

## time-it

### *User exec commands*

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
time-it <LINE>
```

### Parameters

---

<LINE>	Verifies the time taken by a particular command between request and response
	<ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify the command to view the response</li></ul>

---

### Example

```
RFController>time-it enable
That took 0.00 seconds..
RFController#
```

## trace-route

### User exec commands

Traces the route to its defined destination. Use the '-help' or '-h' built in to see a complete list of parameters for the traceroute command.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
trace-route <LINE>
```

### Parameters

---

<LINE>	Traces the route to a destination IP address or a hostname
--------	--

---

### Example

```
RFController>traceroute --help
BusyBox v1.14.1 () multi-call binary

Usage: traceroute [-Fildnr] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q
nqueries]
        [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
        [-z pausesecs] HOST [data size]

Trace the route to HOST

Options:
  -F          Set the don't fragment bit
  -I          Use ICMP ECHO instead of UDP datagrams
  -l          Display the ttl value of the returned packet
  -d          Set SO_DEBUG options to socket
  -n          Print hop addresses numerically rather than symbolically
  -r          Bypass the normal routing tables and send directly to a host
  -v          Verbose
  -m max_ttl  Max time-to-live (max number of hops)
  -p port#    Base UDP port number used in probes
              (default is 33434)
  -q nqueries Number of probes per 'ttl' (default 3)
  -s src_addr IP address to use as the source address
  -t tos      Type-of-service in probe packets (default 0)
  -w wait     Time in seconds to wait for a response
              (default 3 sec)
  -g          Loose source route gateway (8 max)
RFController>traceroute 172.16.10.2
traceroute to 172.16.10.2 (172.16.10.2), 30 hops max, 38 byte packets
 1 172.16.10.1 (172.16.10.1) 3002.008 ms !H 3002.219 ms !H 3003.945 ms !H
```

## watch

### *User exec commands*

Repeats the specific CLI command at a periodic interval

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
watch <1-3600> <LINE>
```

### Parameters

---

<1-3600> <LINE>	Repeats the specified CLI command in the given time intervals. Select a time frame from 1-3600 seconds
-----------------	--

---

### Example

```
RFController>watch 45 page  
RFController>
```

## write

### *User exec commands*

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
write
```

### Parameters

memory	Writes to NV memory
terminal	Writes to terminal

### Example

```
RFController>write memory
[OK]
RFController>
```

```
RFController>write terminal
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
enable
calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
voice-prioritization
svp-prioritization
wmm background cw-max 8
wmm video txop-limit 9
.....RFC
ontroller>
```



## clrscr

### *User exec commands*

Clears the screen and refreshes the prompt (#)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
clrscr
```

### **Parameters**

None

### **Example**

```
RFController>clrscr  
RFController>
```

### exit

#### *User exec commands*

Ends the current mode and moves to the previous mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
exit
```

#### **Parameters**

None

#### **Example**

```
RFController>exit ?  
RFController
```

# Privileged Exec Mode Commands

---

## In this chapter

- [Privileged Exec Mode Commands](#) ..... 67

Most PRIV EXEC commands set operating parameters. Privileged-level access should be password protected to prevent unauthorized use. The PRIV EXEC command set includes commands contained within the USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device followed by a pound sign (#).

To access the PRIV EXEC mode, enter the following at the prompt:

```
RFController>enable
RFController#
```

The PRIV EXEC mode is often referred to as the enable mode, because the enable command is used to enter the mode. There is no provision to configure a password to get access to PRIV EXEC (enable) mode.

---

### NOTE

This chapter contains only those commands which are specific to Privilege Exec Mode only and not present in User Exec Mode. For all other common commands, refer to [Chapter 3, User Exec Mode Commands](#).

---

```
RFController#?
Priv Exec commands:
  ap-upgrade      AP firmware upgrade
  archive         Manage archive files
  boot            Boot commands
  cd              Change current directory
  change-passwd   Change password
  clear           Clear
  clock           Configure software system clock
  cluster         Cluster commands
  commit         Commit all changes made in this session
  configure       Enter configuration mode
  connect         Open a console connection to a remote device
  copy            Copy from one file to another
  crypto          Encryption related commands
  debug           Debugging functions
  delete          Deletes specified file from the system
  diff            Display differences between two files
  dir             List files on a filesystem
  disable         Turn off privileged mode command
  edit            Edit a text file
  enable          Turn on privileged mode command
  erase           Erase a filesystem
  format          Format file system
  halt           Halt the system
```

## 4 In this chapter

help	Description of the interactive help system
logging	Modify message logging facilities
mint	MiNT protocol
mkdir	Create a directory
more	Display the contents of a file
no	Negate a command or set its defaults
page	Toggle paging
ping	Send ICMP echo messages
pwd	Display current directory
reload	Halt and perform a warm reboot
remote-debug	Troubleshoot remote system(s)
rename	Rename a file
revert	Revert changes
rmdir	Delete a directory
self	Config context of the device currently logged into
service	Service Commands
show	Show running system information
telnet	Open a telnet connection
terminal	Set terminal line parameters
time-it	Check how long a particular command took between request and completion of response
tracert	Trace route to destination
upgrade	Upgrade software image
upgrade-abort	Abort an ongoing upgrade
upgrade	Upgrade software image
watch	Repeat the specific CLI command at a periodic interval
write	Write running configuration to memory or terminal
clear	Clears the display screen
exit	Exit from the CLI

RFController#

## Privileged Exec Mode Commands

Table 4 Summarizes the PRIV EXEC commands:

**TABLE 4** PRIV EXEC Commands

Command	Description	Reference
<a href="#">ap-upgrade</a>	Upgrades firmware on access point devices	<a href="#">page 69</a>
<a href="#">archive</a>	Manages file archive operations	<a href="#">page 71</a>
<a href="#">boot</a>	Specifies the image used after reboot	<a href="#">page 72</a>
<a href="#">cd</a>	Changes the current directory	<a href="#">page 73</a>
<a href="#">change-passwd</a>	Changes the password of a logged user	<a href="#">page 74</a>
<a href="#">clear</a>	Clears parameters, cache entries, table entries, and other similar entries	<a href="#">page 75</a>
<a href="#">clock</a>	Configures the system clock	<a href="#">page 78</a>
<a href="#">cluster</a>	Initiates a cluster context	<a href="#">page 80</a>
<a href="#">commit</a>	Commits all the changes made in the current active session	<a href="#">page 82</a>
<a href="#">configure</a>	Enters the configuration mode	<a href="#">page 81</a>
<a href="#">connect</a>	Begins a console connection to a remote device	<a href="#">page 83</a>
<a href="#">copy</a>	Copies a file	<a href="#">page 84</a>
<a href="#">crypto</a>	Enables encryption	<a href="#">page 85</a>
<a href="#">delete</a>	Deletes a specified file from the system	<a href="#">page 95</a>
<a href="#">diff</a>	Displays the differences between 2 files	<a href="#">page 97</a>
<a href="#">dir</a>	Displays the list of files on a file system	<a href="#">page 98</a>
<a href="#">edit</a>	Edits a text file	<a href="#">page 67</a>
<a href="#">enable</a>	Turns on (enables) the privileged mode commands set	<a href="#">page 101</a>
<a href="#">erase</a>	Erases a file system	<a href="#">page 102</a>
<a href="#">format</a>	Formats the file system	<a href="#">page 104</a>
<a href="#">halt</a>	Stops the controller	<a href="#">page 105</a>
<a href="#">help</a>	Describes the interactive help system	<a href="#">page 106</a>
<a href="#">logging</a>	Modified message logging facilities	<a href="#">page 110</a>
<a href="#">mint</a>	Configures MiNT protocols	<a href="#">page 112</a>
<a href="#">mkdir</a>	Creates a new directory in the file system	<a href="#">page 111</a>
<a href="#">more</a>	Displays the contents of a file	<a href="#">page 114</a>
<a href="#">no</a>	Reverts a command or sets values to their default settings	<a href="#">page 115</a>
<a href="#">page</a>	Toggles the Controller paging function.	<a href="#">page 116</a>
<a href="#">ping</a>	Sends ICMP echo messages to a user-specified location	<a href="#">page 117</a>
<a href="#">pwd</a>	Displays the current directory	<a href="#">page 118</a>
<a href="#">reload</a>	Halts the controller and performs a warm reboot	<a href="#">page 119</a>

## 4 Privileged Exec Mode Commands

**TABLE 4** PRIV EXEC Commands

<b>Command</b>	<b>Description</b>	<b>Reference</b>
<a href="#">rename</a>	Renames a file in the existing file system	<a href="#">page 120</a>
<a href="#">revert</a>	Reverts the changes made in the active session	<a href="#">page 121</a>
<a href="#">rmdir</a>	Deletes an existing file from the file system	<a href="#">page 122</a>
<a href="#">self</a>	Displays the configuration context of the device	<a href="#">page 123</a>
<a href="#">service</a>	Performs different functions depending on the parameter passed to it.	<a href="#">page 124</a>
<a href="#">show</a>	Displays the settings for the specified system component	<a href="#">page 125</a>
<a href="#">telnet</a>	Opens a Tel net session	<a href="#">page 127</a>
<a href="#">terminal</a>	Sets the length/number of lines displayed within the terminal window	<a href="#">page 128</a>
<a href="#">time-it</a>	Verifies the time taken by a particular command between request and response	<a href="#">page 129</a>
<a href="#">traceroute</a>	Traces the route to a defined destination.	<a href="#">page 130</a>
<a href="#">upgrade</a>	Upgrades the software image	<a href="#">page 131</a>
<a href="#">upgrade-abort</a>	Aborts an ongoing software image upgrade	<a href="#">page 132</a>
<a href="#">watch</a>	Repeats the specific CLI command at a periodic interval	<a href="#">page 133</a>
<a href="#">write</a>	Writes the system running configuration to memory or terminal	<a href="#">page 134</a>
<a href="#">clrscr</a>	Clears the display screen	<a href="#">page 79</a>
<a href="#">exit</a>	Ends the current CLI session and closes the session window	<a href="#">page 103</a>

## ap-upgrade

### *Privileged Exec Mode Commands*

Enables automatic adopted AP firmware upgrade

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```

ap-upgrade [<DEVICE-NAME>|all|br650|br6511|br6532|br71xx|cancel-upgrade|
load-image|rf-domain]
ap-upgrade [<DEVICE-NAME>|br650|br6511|br6532|br71xx] all {no-reboot/
reboot-time <TIME>/upgrade-time <TIME>}}
ap-upgrade all {no-reboot/reboot-time <TIME>/upgrade-time <TIME>}
ap-upgrade cancel-upgrade [<DEVICE-NAME>|br650|br6511|br6532|br71xx] all
ap-upgrade cancel-upgrade all
ap-upgrade cancel-upgrade on rf-domain [<RF-DOMAINNAME>|all]
ap-upgrade load-image [br650|br6511|br6532|br71xx] <URL>

ap-upgrade rf-domain <rf-domainname> [all|br650|br6511|br6532|
br71xx] {no-reboot/no-via-rf-domain/reboot-time <TIME>/
upgrade-time <TIME>}
ap-upgrade rf-domain all [all|br650|br6511|br6532|br71xx]
{no-reboot/no-via-rf-domain/reboot-time <TIME>/upgrade-time <TIME>}

```

## Parameters

- 
- [<DEVICE-NAME> | all | br650 | br71xx | br6511 | br6532 ] [ cancel-upgrade | load-image | rf-domain ]
- <DEVICE-NAME> all {no-reboot | reboot-time <TIME> | upgrade-time <TIME>} - Specify the name/MAC address of an AP
  - all {no-reboot | reboot-time <TIME> | upgrade-time <TIME>} - Upgrades all the access points
  - br650 all {no-reboot | reboot-time <TIME> | upgrade-time <TIME>} - Upgrades a br650 device
  - br6511 all {no-reboot | reboot-time <TIME> | upgrade-time <TIME>} - Upgrades a br6511 device
  - br6532 all {no-reboot | reboot-time <TIME> | upgrade-time <TIME>} - Upgrades a br6532 device
  - br71xx all {no-reboot | reboot-time <TIME> | upgrade-time <TIME>} - Upgrades a br71xx device
  - cancel-upgrade [<DEVICE-NAME> | br650 | br6532 | br71xx | br6511 | all] - Cancels upgrading the AP
  - load-image [br650 | br71xx | br6511] <URL> - Loads the AP firmware images on the Controller
    - <URL> - Specify the location of firmware image

URLs: tftp://<hostname | IP>[:port]/path/file  
 ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file  
 sftp://<user>:<passwd>@<hostname | IP>[:port]/path/file  
 http://<hostname | IP>[:port]/path/file  
 cf:/path/file  
 usb1:/path/file  
 usb2:/path/file
  - rf-domain <RF-DOMAINNAME> {no-reboot | no-via-rf-domain | reboot-time <TIME> | upgrade-time <TIME>} - Upgrades all the access points belonging to an RF Domain
    - no-via-rf-domain - Upgrades APs from the adopted device
- The following are common for all the above:
- no-reboot - No reboot (manually reboot after the upgrade)
  - reboot-time <TIME> - Sets the scheduled reboot time
  - upgrade-time <TIME> - Sets the scheduled upgrade time
    - <TIME> - Specify the reboot time in MM/DD/YYYY-HH:MM or HH:MM format
- 

## Example

```
RFController>ap-upgrade br650 00-A0-F8-00-00-00
RFController>
RFController>ap-upgrade all
RFController>
RFController>ap-upgrade default/rfs4000-880DA7 no-reboot
-----
CONTROLLER          STATUS          MESSAGE
-----
00-23-68-88-0D-A7   Success        Queued 0 APs to upgrade
-----
RFController>
RFController#ap-upgrade RFController reboot-time 06/01/2011-12:10
-----
CONTROLLER          STATUS          MESSAGE
-----
00-15-70-37-FA-BE   Success        Queued 0 APs to upgrade
-----
---
RFController#
```



## archive

### *Privileged Exec Mode Commands*

Manages file archive operations

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
archive tar /table [<FILE>|<URL>]
archive tar /create [<FILE>|<URL>] <FILE>
archive tar /xtract [<FILE>|<URL>] <DIR>
```

### Parameters

tar	Manipulates (creates, lists or extracts) a tar file
/table	Lists the files in a tar file
/create	Creates a tar file
/xtract	Extracts content from a tar file
<FILE>	Defines a Tar filename
<URL>	Sets the tar file URL
<DIR>	A directory name. When used with /create, the dir is the source directory for the tar file. When used with /xtract, the dir is the destination file where the contents of the tar file are extracted.

### Example

How to zip the folder flash:/log/?

```
RFController#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
RFController#dir flash:/
```

### boot

#### *Privileged Exec Mode Commands*

Specifies the image used after reboot

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
boot system [primary|secondary] {on <DEVICE-NAME>}
```

#### Parameters

---

system [primary secondary] {on <DEVICE-NAME>}	Specifies the image to be used after a device reboot
	<ul style="list-style-type: none"><li>• primary – Primary image used after reboot</li><li>• secondary – Secondary image used after reboot<ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li><li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li></ul></li></ul>

---

#### Example

```
RFController#boot system primary on RFController
Rebooting with primary partition
RFController#
```

## cd

### *Privileged Exec Mode Commands*

Changes the current directory

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
cd {<DIR>}
```

### Parameters

---

<DIR>	Changes the current directory to DIR. This parameter is optional. When this parameter is not provided, the current directory name is displayed.
-------	---

---

### Example

```
RFController#cd
nvram:/  system:/  flash:/

RFController#cd flash:/?
DIR Change current directory to DIR

RFController#cd flash:/
flash:/backup/      flash:/crashinfo/  flash:/hotspot/      flash:/log/
flash:/out/

RFController#cd flash:/log/?
DIR Change current directory to DIR

RFController#cd flash:/log/
RFController#pwd
flash:/log/
RFController#
```

## change-passwd

### *Privileged Exec Mode Commands*

Changes the password of the logged in user

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
change-passwd {<OLD-PASSWD> <NEW-PASSWD>}
```

### Parameters

---

{<OLD-PASSWD>  
<NEW-PASSWD>}

Optional. The passwords can also be changed interactively. To do so, press Enter after the change-passwd command.

- <OLD-PASSWD> - The password needing to be changed
  - <NEW-PASSWD> - The new password to update to.
- 

### Usage Guidelines

A password must be between 8 to 32 characters in length.

### Example

```
RFController#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
Please write this password change to memory(write memory) to be persistent.
RFController>write memory
OK
RFController>
```

## clear

### *Privileged Exec Mode Commands*

Clears parameters, cache entries, table entries, and other similar entries. The clear command is only available for specific commands. The information cleared using this command varies depending on the mode where the clear command is executed.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

---

### NOTE

Refer to the interface details below when using `clear`

- `ge <index>` - RFS4000 supports 4GEs and RFS6000 supports 8 GEs

- `me1` - Available in both RFS7000 and RFS6000

---

### Syntax

```
clear [arp-cache|cdp|counters|crypto|event-history|firewall|ip|lldp|
      spanning-tree]
clear arp-cache {on <DEVICE-NAME>}
clear [cdp|lldp] neighbors {on <DEVICE-NAME>}
clear crypto [ipsec|isakmp] sa [<IP>|all] {on <DEVICE-NAME>}
clear event-history
clear firewall [dhcp snoop-table|dos stats|flows] {on <DEVICE-NAME>}
clear ip dhcp bindings [<A.B.C.D>|all] {on <DEVICE-NAME>}
clear spanning-tree detected-protocols {interface {<INTERFACE>|
      ge <1-8>|me1|port-channel <1-4>|vlan <1-4094>} {on <DEVICE-NAME>}}

clear counters [all|bridge|router|thread]
clear counters interface [<INTERFACE>|all|ge <1-8>|me1|
      port-channel <1-4>|vlan <1-4094>]
```

## 4 Privileged Exec Mode Commands

### Parameters

arp-cache {on <DEVICE-NAME>}	<p>Clears ARP cache entries.</p> <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the arp cache on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul>
[cdp lldp] neighbors {on <DEVICE-NAME>}	<p>Clears Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) neighbor table entries</p> <ul style="list-style-type: none"> <li>neighbors – Clears CDP neighbor table <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul> </li> </ul>
clear counters [all bridge router thread] clear counters interface [<INTERFACE> all  ge <1-8> me1] port-channel <1-4> vlan <1-4094>]	<p>Clears the different counters available on the system.</p> <ul style="list-style-type: none"> <li>all – Clears all counters</li> <li>bridge – Clears the bridge counters</li> <li>router – Clears the router counters</li> <li>thread – Clears the thread counters</li> <li>interface [&lt;INTERFACE&gt; all ge &lt;1-8&gt; me1 port-channel &lt;1-4&gt; vlan &lt;1-4094&gt;] – Clears the interface counters for the specified interface.</li> </ul>
crypto [ipsec isakmp] sa [<IP> all] {on <DEVICE-NAME>}	<p>Clears the encryption module's databases.</p> <ul style="list-style-type: none"> <li>ipsec sa – Clears the IPSEC security associations.</li> <li>isakmp sa – Clears the ISAKMP security associations.</li> </ul> <p>The following are common for the above:</p> <ul style="list-style-type: none"> <li>&lt;IP&gt; – Clears the IPsec or ISAKMP security associations for a certain Peer.</li> <li>all – Clears the IPsec or ISAKMP security associations for all Peers. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the SAs on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul> </li> </ul>
event-history	Clears event history
firewall [dhcp snoop-table dos stats flows] {on <DEVICE-NAME>}	<p>Clears the firewall event entries.</p> <ul style="list-style-type: none"> <li>dhcp snoop-table – Clears the DHCP Snoop Table entries</li> <li>dos stats – Clears the denial of service statistics</li> <li>flows – Clears the established firewall sessions. <ul style="list-style-type: none"> <li>on &lt;DEVICE-NAME&gt; – Optional. Clears the SAs on a selected AP or Controller</li> <li>&lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul> </li> </ul>

---

<pre>ip dhcp bindings [&lt;IP all&gt;] {on &lt;DEVICE-NAME&gt;}</pre>	<p>Clears the DHCP address bindings.</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller</li> <li>• &lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul>
<pre>spanning-tree detected-protocols {interface &lt;INTERFACE&gt; ge &lt;1-8&gt; me1 port-channel &lt;1-4&gt; vlan &lt;1-4094&gt;} {on &lt;DEVICE-NAME&gt;}</pre>	<p>Clears the spanning-tree protocols configured for the interface</p> <ul style="list-style-type: none"> <li>• detected-protocols {interface [&lt;INTERFACE&gt; ge &lt;1-8&gt; me1 port-channel &lt;1-4&gt; vlan &lt;1-4094&gt;]} {on} – Enter the interface name to clear the detected spanning tree protocols for that specific interface <ul style="list-style-type: none"> <li>• &lt;INTERFACE&gt; – Clears the selected interface name</li> <li>• ge &lt;1-8&gt; – Clears the configured GigabitEthernet interface status</li> <li>• me1 – Clears the FastEthernet interface status</li> <li>• port-channel &lt;1-4&gt; – Clears the port-channel information on a AP/Controller</li> <li>• vlan &lt;1-4094&gt; – Clears the configured vlan information</li> <li>• wwan1 – Clears the Wireless WAN interface information</li> </ul> </li> </ul> <p>The following are common for the above</p> <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Optional. Clears the CDP/LLDP neighbor table entries on a selected AP or Controller</li> <li>• &lt;DEVICE-NAME&gt; – An AP or a Controller name</li> </ul>

---

### Example

```
RFController#clear crypto isakmp sa 111.222.333.01 on RFController
RFController#

RFController#clear event-history
RFController#

RFController#clear firewall dos stats on RFController
RFController#

RFController#clear spanning-tree detected-protocols interface port-channel 1
on RFController
RFController#

RFController#clear ip dhcp bindings 172.16.10.9 on RFController
RFController#

RFController#clear cdp neighbors on RFController
RFController#
rfs4000-880DA7#clear spanning-tree detected-protocols interface ge 1
rfs4000-880DA7#

rfs4000-880DA7#clear lldp neighbors
rfs4000-880DA7#
```

### clock

#### *Privileged Exec Mode Commands*

Configures the system clock

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
clock set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>}
```

#### Parameters

- 
- |  |   |
|--|---|
| set <HH:MM:SS> <1-31> <MONTH> <1993-2035> {on <DEVICE-NAME>} | <ul style="list-style-type: none"><li>• Sets the software system clock for the configured device<ul style="list-style-type: none"><li>• &lt;HH:MM:SS&gt; – Sets the current time (in military format hours, minutes and seconds)</li><li>• &lt;1-31&gt; – Enter the numerical day of the month<ul style="list-style-type: none"><li>• &lt;MONTH&gt; – Enter the month of the year (Jan to Dec)</li><li>• &lt;1993-2035&gt; – Select a valid digit year from 1993-2035</li><li>• on – On AP/Controller</li><li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li></ul></li></ul></li></ul> |
|--|---|
- 

#### Example

```
RFController#clock set 12:30:45 2 MONTH 2010 on RFController
clock set 12:30:45 2 MONTH 2010 on RFController RFController>
```



## clrscr

### *Privileged Exec Mode Commands*

Clears the screen and refreshes the prompt (#)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
clrscr
```

### **Parameters**

None

### **Example**

```
RFController#clrscr  
RFController#
```

## cluster

### *Privileged Exec Mode Commands*

Use this command to initiate the cluster context. The cluster context provides centralized management to configure all the cluster members from any one member.

Any commands executed under this context are executed on all members of the cluster.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
cluster start-selection
```

### Parameters

---

start-selection	Starts a new cluster master election
-----------------	--------------------------------------

---

### Example

```
RFController#cluster start-election  
RFController#
```

## configure

### *Privileged Exec Mode Commands*

Enters the configuration mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
configure {self|terminal}
```

### Parameters

self	Enables configuration from the terminal
terminal	Enables the configuration mode of the current device

### Example

```
RFController#configure self
Enter configuration commands, one per line. End with CNTL/Z.
RFController(config-device-00-15-70-37-FA-BE)#
```

```
RFController#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RFController(config)#
```

### commit

#### *Privileged Exec Mode Commands*

Commits all the changes made in the active session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
commit {write memory}
```

#### Parameters

---

write memory	If a commit succeeds, the configuration is written to memory
	<ul style="list-style-type: none"><li>• memory - Writes the changes to memory</li></ul>

---

#### Example

```
RFController#commit write memory
[OK]
RFController#
```

## connect

### *Privileged Exec Mode Commands*

Begins a console connection to a remote device using the remote device's MINT ID or its device name.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
connect [mint-id <MINT-ID> | <REMOTE-DEVICE-NAME>]
```

### Parameters

mint-id <MINT-ID>	Connects to the remote system using MINT ID. <ul style="list-style-type: none"> <li>• &lt;MINT-ID&gt; - The MINT ID of the remote device.</li> </ul>
<REMOTE-DEVICE-NAME>	Connects to the remote system using its device name.

### Example

```
RFController#connect RFDOMAIN_UseCase1/rfs7000

Entering character mode
Escape character is '^]'.
RFS7000 release 5.1.0.0
RFController login: admin
Password:
Welcome to CLI
RFController>
```

## copy

### Privileged Exec Mode Commands

Copies file (config,log,txt ...etc) from any location to the controller and vice-versa

---

#### NOTE

Copying a new config file onto an existing running-config file merges it with the existing running-config on the controller. Both the existing running-config and the new config file are applied as the current running-config.

Copying a new config file onto a start-up config files replaces the existing start-up config file with the parameters of the new file. It is better to erase the existing start-up config file and then copy the new config file to the startup config.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
copy [FILE|URL] [FILE|URL]
```

#### Parameters

---

FILE	The first <FILE> is the source file to copy from. The second <FILE> is the destination to copy.
URL	The first <URL> is the source URL to copy from. The second <URL> is the destination URL to copy.

---

#### Example

Transferring file snmpd.log to remote tftp server?

```
RFController#copy flash:/log/snmpd.log  
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switchrunning-config?

```
RFController#copy tftp://157.235.208.105:/running-config running-config
```

## crypto

### Privileged Exec Mode Commands

Enables encryption

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
crypto [key|pki]

crypto key [export|generate|import|zeroise]
crypto key export rsa <RSA-KEYPAIR-NAME>> <EXPORT-TO-URL>
    {background|on|passphrase}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL>
    {background} {on <DEVICE-NAME>}
crypto key export rsa <RSA-KEYPAIR-NAME> <EXPORT-TO-URL> {passphrase
<KEY-PASSPHRASE>} {background} {on <DEVICE-NAME>}

crypto key generate rsa <RSA-KEYPAIR-NAME> <1024-2048>
    {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL>
    {background} {on <DEVICE-NAME>}

crypto key import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> passphrase
<KEY-PASSPHRASE> {background} {on <DEVICE-NAME>}

crypto key zeroise rsa <RSA-KEYPAIR-NAME> {force} {on <DEVICE-NAME>}

crypto pki [authenticate|export|generate|import|zeroise]
crypto pki authenticate <TRUST-POINT> <URL> {background} {on <DEVICE-NAME>}

crypto pki export [request|trustpoint]
crypto pki export request [generate-rsa-key|use-rsa-key]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
[autogen-subject-name|subject-name]
crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name (<EXPORT-TO-URL> ,email <SEND-TO-EMAIL> ,fqdn
<FQDN> ,ip-address <IP>)

crypto pki export request [generate-rsa-key|use-rsa-key] <RSA-KEYPAIR-NAME>
autogen-subject-name <EXPORT-TO-URL> {background} {on <DEVICE-NAME>}

crypto pki export request [generate-rsa-key|use-rsa-key] <WORD> subject-name
<COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANISATION> <ORGANIZATION-UNIT>
[<EXPORT-TO-URL>|email <SEND-TO-EMAIL>|fqdn <FQDN>|ip-address <IP>]
```

## 4 Privileged Exec Mode Commands

```
crypto pki export trustpoint <TRUSTPOINT-NAME> <EXPORT-TO-URL> {{background}
{on <DEVICE--NAME>}/passphrase <KEY-PHRASE> {background} {on <DEVICE-NAME>}/on
<DEVICE-NAME>}}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> [autogen-subject-name|subject-name]
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name
{email/fqdn/ip-address/on}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name email <WORD> {fqdn
<WORD>}/ip-address <A.B.C.D>/on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name fqdn <WORD> {email
<WORD>}/ip-address <A.B.C.D>/on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name ip-address
<A.B.C.D> {fqdn <WORD>/on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> autogen-subject-name {on <DEVICE-NAME>}
```

```
crypto pki generate self-assigned <TRUSTPOINT-NAME>
[generate-rsa-key|use-rsa-key] <WORD> subject-name <COMMON-NAME> <COUNTRY>
<STATE> <CITY> <ORGANISATION> <ORGANIZATION-UNIT> {email <WORD>/fqdn
<WORD>}/ip-address <A.B.C.D>/on} <DEVICE-NAME>
```

```
crypto pki import [certificate|crl|trustpoint]
```

```
crypto pki import [certificate|crl] <WORD> <IMPORT-FROM-URL> {background {on
<DEVICE-NAME>}/on <DEVICE--NAME>}}
```

```
crypto pki import trustpoint <TRUSTPOINT-NAME> <IMPORT-FROM-URL> {background
{on <DEVICE-NAME>}/on <DEVICE-NAME>/passphrase <word> {background {on
<DEVICE-NAME>}/on <DEVICE-OR-DOMAIN-NAME>}
```

```
crypto pki zeroise trustpoint <TRUSTPOINT-NAME> {del-key {on
<DEVICE-OR-DOMAIN-NAME>}/on <DEVICE-NAME>}
```



**Parameters**

key	Performs key management operations
key export	<ul style="list-style-type: none"> <li>• export rsa &lt;RSA-KEYPAIR-NAME&gt; &lt;EXPORT-TO-URL&gt; {background   on   phrase} – Performs export operation <ul style="list-style-type: none"> <li>• rsa &lt;RSA-KEYPAIR-NAME&gt; – Enter the name of a RSA keypair to export <ul style="list-style-type: none"> <li>• &lt;EXPORT-TO-URL&gt; {background   on   phrase} – Enter the location to send the key to using the following syntax:  tftp://&lt;hostname   IP&gt;[:port]/path/file  ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname   IP&gt;[:port]/path/file  sftp://&lt;user&gt;@&lt;hostname   IP&gt;[:port]/path/file  http://&lt;hostname   IP&gt;[:port]/path/file  cf:/path/file  usb1:/path/file  usb2:/path/file <ul style="list-style-type: none"> <li>• background {on &lt;DEVICE-NAME&gt;} – Performs the operation in background</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> <li>• passphrase &lt;KEY-PASSPHRASE&gt; {background   on } – Enter a passphrase to encrypt the RSA key (aes-128)</li> <li>• background {on &lt;DEVICE-NAME&gt;} – Performs the operation in the background</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> </li> </ul> </li> </ul> </li> </ul>
key generate	<ul style="list-style-type: none"> <li>• generate rsa &lt;RSA-KEYPAIR-NAME&gt; &lt;1024-2048&gt; {on &lt;DEVICE-NAME&gt;} – Generates a keypair <ul style="list-style-type: none"> <li>• rsa &lt;WORD&gt; – Enter the name of a RSA keypair to generate <ul style="list-style-type: none"> <li>• &lt;1024-2048&gt; – Enter the size of the RSA key in bits from 1024-2048</li> <li>• on &lt;DEVICE-NAME&gt; – On an AP or a Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> </li> </ul> </li> </ul>

---

key import

- import rsa <RSA-KEYPAIR-NAME> <IMPORT-FROM-URL> {background {on <DEVICE-NAME>}} | on <DEVICE-NAME> } | passphrase} - Performs an import operation
  - rsa <RSA-KEYPAIR-NAME> - Enter the name of a RSA keypair to import
    - <IMPORT-FROM-URL> {background | on | phrase} - Enter the location to send the key using the following formats:  
 tftp://<hostname | IP>[:port]/path/file  
 ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file  
 sftp://<user>@<hostname | IP>[:port]/path/file  
 http://<hostname | IP>[:port]/path/file  
 cf:/path/file  
 usb1:/path/file  
 usb2:/path/file
    - background {on <DEVICE-NAME>} - Performs the operation in the background
    - on <DEVICE-NAME> - On AP/Controller
    - <DEVICE-NAME> - On AP/Controller name
    - on <DEVICE-NAME> - On AP/Controller
    - <DEVICE-NAME> - On AP/Controller name
    - passphrase <KEY-PASSPHRASE>> {background | on} - Enter a passphrase to decrypt the RSA key (aes-128)
    - background {on <DEVICE-NAME>} - Performs the operation in background
    - on <DEVICE-NAME> - On an AP or a Controller

---

key zeroize

- zeroize rsa <RSA-KEYPAIR-NAME> {force {on <DEVICE-OR-DOMAIN-NAME>}} | on <DEVICE-NAME>} - Performs delete operation
  - rsa <RSA-KEYPAIR-NAME> - Deletes the specified RSA key
    - force {on <DEVICE-NAME>} - Forces the deletion of all certificates associated with the key
      - on <DEVICE-NAME> - On AP/Controller
      - <DEVICE-NAME> - On AP/Controller name
      - on <DEVICE-NAME> - On AP/Controller
      - <DEVICE-NAME> - On AP/Controller name

---

pki [authenticate | export | generate | import | zeroize] Performs PKI related commands

---

pki authenticate <trustpoint-name> <URL> {background} {on <DEVICE-name>}

- authenticate <TRUSTPOINT-NAME> - Authenticates and imports ca certificate
  - <URL> (background | on) - Enter the location of ca certificate to authenticate  
 tftp://<hostname | IP>[:port]/path/file  
 ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file  
 sftp://<user>@<hostname | IP>[:port]/path/file  
 http://<hostname | IP>[:port]/path/file  
 cf:/path/file  
 usb1:/path/file  
 usb2:/path/file
  - {background} {on <DEVICE-NAME>} - Performs the operation in the background
    - on <DEVICE-NAME> - On AP/Controller
    - <DEVICE-NAME> - On AP/Controller name
    - on <DEVICE-NAME>} - On AP/Controller
    - <DEVICE-NAME> - On AP/Controller name

- 
- ```
crypto pki export request
[generate-rsa-key | use-rsa-key]
<RSA-KEYPAIR-NAME>
[autogen-subject-name | subject-
name]
```
- export – Performs export operation
    - request [generate-rsa-key | use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] [<EXPORT-TO-URL> | email | fqdn | ip-address] – Generates and exports a Certificate Signing Request
      - generate-rsa-key <RSA-KEYPAIR-NAME> – Generates a new RSA key-pair
      - use-rsa-key – Uses a generated RSA key-pair

The following parameters are common for the above:

- RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] – Enter the name of RSA key-pair to export
- autogen-subject-name – Autogenerates the subject name from config parameters
- URL – Enter the URL to export the CSR
  - fttp://<hostname | IP>[:port]/path/file
  - ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file
  - sftp://<user>@<hostname | IP>[:port]/path/file
  - http://<hostname | IP>[:port]/path/file
  - cf:/path/file
  - usb1:/path/file
  - usb2:/path/file
- email – Enter the email address
- fqdn – Enter the fully qualified domain name
- ip-address – Enter the IP Address

- 
- subject-name <COMMON-NAME> <COUNTRY> <STATE> <CITY> <ORGANIZATION> <ORGANIZATION-UNIT> {email <EMAIL> | fqdn <FQDN> | ip-address <IP> | on <DEVICE-OR-DOMAIN-NAME>} – Enter the subject name to identify the certificate
  - <COMMON-NAME> – Enter the common name to be used with the ca certificate
  - <COUNTRY> – Enter the deployment country (2 character ISO code)
  - <STATE> – Enter the state (2 to 64 characters)
  - <CITY> – Enter the city (2 to 64 characters)
  - <ORGANIZATION> – Enter the organization name (2 to 64 characters)
  - <ORGANIZATION-UNIT> – Enter the organization unit name (2 to 64 characters)
  - email <WORD> – Enter the email address
  - fqdn – Enter the fully qualified domain name
  - ip-address <A.B.C.D> – Enter the IP Address
  - on <DEVICE-NAME> – On AP/Controller
  - <DEVICE-NAME> – AP/Controller name

## 4 Privileged Exec Mode Commands

---

```
export trustpoint
<TRUSTPOINT-NAME>
<EXPORT-TO-URL>
{background} {on}
<DEVICE-NAME>
```

Exports a trustpoint (CA cert, CRL server cert and private key).

- <TRUSTPOINT-NAME> – Enter the trust point name
- <EXPORT-TO-URL> (background|on) – Enter the location of ca certificate to import

URLs: tftp://<hostname|IP>[:port]/path/file

ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

sftp://<user>@<hostname|IP>[:port]/path/file

http://<hostname|IP>[:port]/path/file

cf:/path/file

usb1:/path/file usb2:/path/file

- background {on <DEVICE-NAME>} – Performs the operation in background
- on <DEVICE-NAME> – On AP/Controller
- <DEVICE-NAME> – On AP/Controller name
- on <DEVICE-NAME>} – On AP/Controller
- <DEVICE-NAME> – On AP/Controller name

- 
- generate self-signed  
<TRUSTPOINT-NAME>  
[generate-rsa-key | use-rsa-key]  
<RSA-KEYPAIR-NAME>
- generate self-assigned <TRUSTPOINT-NAME> [generate-rsa-key | use-rsa-key] <RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] - Generates Operation
    - self-assigned - Generates a self-signed certificate (and trustpoint with it)
      - <TRUSTPOINT-NAME> [generate-rsa-key | use-rsa-key] - Enter the trust point name
        - generate-rsa-key - Generates a new RSA key-pair
        - use-rsa-key - Uses a generated RSA key-pair

The following parameters are common for the above:

- <RSA-KEYPAIR-NAME> [autogen-subject-name | subject-name] - Enter the name of RSA key-pair to export
- autogen-subject-name - Autogenerates the subject name from config parameters
- URL - Enter the URL to export the CSR to  
URLs: tftp://<hostname | IP>[:port]/path/file  
ftp://<user>:<passwd>@<hostname | IP>[:port]/path/file  
sftp://<user>@<hostname | IP>[:port]/path/file  
http://<hostname | IP>[:port]/path/file  
cf:/path/file  
usb1:/path/file  
usb2:/path/file
- email - Enter a destination email address
- fqdn - Enter the fully qualified domain name
- ip-address - Enter an IP Address
- subject-name <Common-Name> <Country> <State> <City> <Organization> <Organization-Unit> {email<WORD> | fqdn <WORD> | ip-address <A.B.C.D> | on} <DEVICE-OR-DOMAIN-NAME> - Enter the subject name to identify the certificate
- <Common-Name> - Enter the common name used with the certificate
- <Country> - Enter the country (2 character ISO code)
- State - Enter the state (2 to 64 characters)
- City - Enter the city (2 to 64 characters)
- <Organization> - Enter the Organization name (2 to 64 characters)
- <Organization-Unit> {email <WORD> | fqdn <WORD> | ip-address <A.B.C.D> | on} - Enter the Organization unit name (2 to 64 characters)
- email <WORD> - Enter the email address
- fqdn - Enter the fully qualified domain name
- ip-address <A.B.C.D> - Enter the IP Address
- on <DEVICE-NAME> - On AP/Controller
- <DEVICE-NAME> - AP/Controller name

## 4 Privileged Exec Mode Commands

---

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| import<br>[certificate   crl   trustpoint] | <p>Imports certificates, certificate revocation list or a trustpoint to the selected device.</p> <ul style="list-style-type: none"><li>• certificate &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt; {background} {on &lt;DEVICE-NAME&gt;}   on &lt;DEVICE-NAME&gt; - Imports the signed server certificate<ul style="list-style-type: none"><li>• &lt;TRUSTPOINT-NAME&gt; - Enter the name of the trustpoint (should be already authenticated)<ul style="list-style-type: none"><li>• &lt;IMPORT-FROM-URL&gt; - Enter the URL to import from<br/>URLs: tftp://&lt;hostname   IP&gt;[:port]/path/file<br/>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname   IP&gt;[:port]/path/file<br/>sftp://&lt;user&gt;@&lt;hostname   IP&gt;[:port]/path/file<br/>http://&lt;hostname   IP&gt;[:port]/path/file<br/>cf:/path/file<br/>usb1:/path/file<br/>usb2:/path/file</li></ul></li></ul></li><li>• crl &lt;TRUSTPOINT-NAME&gt; &lt;IMPORT-FROM-URL&gt; {background} {on &lt;DEVICE-NAME&gt;}   on &lt;DEVICE-NAME&gt; - Imports a Certificate revocation list<ul style="list-style-type: none"><li>• &lt;TRUSTPOINT-NAME&gt; - Enter the name of trustpoint to which CRL belongs<ul style="list-style-type: none"><li>• &lt;IMPORT-FROM-URL&gt; - URL to import CRL from<br/>URLs: tftp://&lt;hostname   IP&gt;[:port]/path/file<br/>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname   IP&gt;[:port]/path/file<br/>sftp://&lt;user&gt;@&lt;hostname   IP&gt;[:port]/path/file<br/>http://&lt;hostname   IP&gt;[:port]/path/file<br/>cf:/path/file<br/>usb1:/path/file<br/>usb2:/path/file</li></ul></li></ul></li></ul> <p>The following parameters are common for certificate and crl:</p> <ul style="list-style-type: none"><li>• background {on &lt;DEVICE-NAME&gt;} - Performs the operation in background</li><li>• on &lt;DEVICE-NAME&gt; - On AP/Controller</li><li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li><li>• on &lt;DEVICE-NAME&gt;} - On AP/Controller</li><li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li></ul> |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 
- `trustpoint <WORD> URL {background {on <DEVICE-OR-DOMAIN-NAME>} | on <DEVICE-NAME> | passphrase <word> {background {on <DEVICE-NAME>} | on <DEVICE-NAME>}} - Imports a trustpoint, includes CA certificate, server certificate and private key`
  - `<WORD>` - Enter the name of the trustpoint name
    - `URL {background | on}` - Enter the location to import trustpoint from

URLs: `tftp://<hostname|IP>[:port]/path/file`  
`ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file`  
`sftp://<user>@<hostname|IP>[:port]/path/file`  
`http://<hostname|IP>[:port]/path/file`  
`cf:/path/file`  
`usb1:/path/file usb2:/path/file`

    - `background {on <DEVICE-NAME>}` - Performs the operation in the background
    - `on <DEVICE-NAME>` - On AP/Controller
    - `<DEVICE-NAME>` - On AP/Controller name
    - `on <DEVICE-NAME>` - On AP/Controller
    - `<DEVICE-OR-DOMAIN-NAME>` - On AP/Controller name
    - `passphrase <WORD> {background | on}` - Enter a passphrase if the private key is to be exported encrypted)
    - `background {on <DEVICE-NAME>}` - Performs the operation in the background
  - `zeroize trustpoint <TRUSTPOINT-NAME> {del-key} {on <DEVICE-NAME>}` - Performs delete operation
    - `trustpoint <WORD>` - Enter the name of the trustpoint to delete
      - `del-key {on <DEVICE-NAME>}` - Deletes the private key associated to the server certificate
        - `on <DEVICE-NAME>` - On AP/Controller
        - `<DEVICE-NAME>` - On AP/Controller name
- 

### Example

```
RFController>crypto key generate rsa key 1025
RSA Keypair successfully generated
RFController>
```

```
RFController>crypto key import rsa admin123 url passphrase word background on
RFController
RSA key import operation is started in background
RFController>
```

```
RFController>crypto pki generate self-signed word generate-rsa-key word
autogen-subject-name fqdn word
Successfully generated self-signed certificate
RFController>
```

```
RFController#crypto pki zeroize trustpoint word del-key on RFController
Successfully removed the trustpoint and associated certificates
%Warning: Applications associated with the trustpoint will start using
default-trustpoint
RFController#
```

```
RFController>crypto pki authenticate word url background on RFController
Import of CA certificate started in background
RFController>
```

## 4 Privileged Exec Mode Commands

```
RFController>crypto pki import trustpoint word url passphrase word on
RFController
Import operaton started in background
RFController>
```



## delete

### *Privileged Exec Mode Commands*

Deletes a specified file from the system

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
delete [/force <FILE>|/recursive <FILE>|<FILE>]
```

### Parameters

|            |                                     |
|------------|-------------------------------------|
| /force     | Forces deletion without a prompt    |
| /recursive | Performs a recursive delete         |
| <FILE>     | Specifies the filename(s) to delete |

### Example

```
RFController#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

RFController#delete /force flash:/tmp.txt
RFController#

RFController#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
RFController#
```

### disable

#### *Privileged Exec Mode Commands*

Turns off (disables) the privileged mode command set. This command is not applicable to the User Executable mode.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
disable
```

#### **Parameters**

None

#### **Example**

```
RFController>disable  
RFController>
```

## diff

### *Privileged Exec Mode Commands*

Displays the differences between 2 files

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
diff [<FILE>|<URL>] [<FILE>|<URL>]
```

### Parameters

|      |                                                                                             |
|------|---------------------------------------------------------------------------------------------|
| FILE | The first <FILE> is the source file for the diff. The second <FILE> is the file to compare. |
| URL  | The first <URL> is the source URL for the diff. The second <URL> is the url to compare.     |

### Example

```
RFController#diff startup-config running-config
--- startup-config
+++ running-config
@@ -1,3 +1,4 @@
+!### show running-config
!
! Configuration of RFS7000 version 5.1.0.0
!
@@ -80,7 +81,6 @@
  excluded-address 172.16.10.9 172.16.10.10
  bootp ignore
!
-gui default
!
  firewall-policy default
!
RFController#
```

## dir

### Privileged Exec Mode Commands

Use this command to view the list of files on a filesystem

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
dir {[/all|/recursive|<DIR>|all-file systems]}
```

### Parameters

|                  |                                    |
|------------------|------------------------------------|
| /all             | Lists all files                    |
| /recursive       | Lists files recursively            |
| <DIR>            | Lists files in the named file path |
| all-file systems | Lists the files on all filesystems |

### Example

```
RFController# dir
Directory of flash:/.

drwx          Thu Apr 29 12:36:29 2010  log
-rw-   39     Tue Dec 29 11:41:00 2009  FILE
drwx          Thu Apr 29 11:34:11 2010  crashinfo
drwx          Sat Jan  1 00:00:25 2000  hotspot
drwx          Mon Dec 14 14:09:39 2009  TestDir
drwx          Fri Dec 11 15:38:25 2009  Testdir

RFController#

RFController#dir all-file systems
Directory of flash:/

drwx          Thu Apr 29 12:36:29 2010  log
-rw-   39     Tue Dec 29 11:41:00 2009  FILE
drwx          Thu Apr 29 11:34:11 2010  crashinfo
drwx          Sat Jan  1 00:00:25 2000  hotspot
drwx          Mon Dec 14 14:09:39 2009  TestDir
drwx          Fri Dec 11 15:38:25 2009  Testdir

Directory of nvram:/

-rw-   3460    Fri Dec 11 14:42:44 2009  startup-config.save
-rw-   1638    Tue Jan  5 14:27:17 2010  startup-config-unused
-rw-   3393    Mon Dec 14 13:55:51 2009  startup-config.save.1
```

```
-rw- 8059 Thu Apr 29 12:36:27 2010 startup-config
Directory of system:/
drwx Thu Apr 29 12:35:52 2010 proc
RFController#
```

## edit

### *Privileged Exec Mode Commands*

Edits a text file

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
edit <FILE>
```

### Parameters

---

|        |                                 |
|--------|---------------------------------|
| <FILE> | Name of the file to be modified |
|--------|---------------------------------|

---

### Example

```
RFController#edit startup-config
GNU nano 1.2.4                                     File: startup-config

!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
  enable
  calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
  voice-prioritization
  svp-prioritization
  wmm background cw-max 8
  wmm video txop-limit 9
  wmm voice cw-min 6
  wmm voice cw-max 6
  rate-limit client to-air max-burst-size 3
  rate-limit client to-air red-threshold video 101
  rate-limit client from-air rate 55
  rate-limit client from-air red-threshold background 100
  rate-limit client from-air red-threshold voice 1010
!
!
```

## enable

### *Privileged Exec Mode Commands*

Turns on (enables) the privileged mode command set. This command is not applicable in the Privileged Executable mode.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
enable
```

### **Parameters**

None

### **Example**

```
RFController>enable  
RFController#
```

## erase

### *Privileged Exec Mode Commands*

Erases a filesystem

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
erase [cf:|flash:|nvram:|startup-config|usb1]
```

### Parameters

|                |                                        |
|----------------|----------------------------------------|
| cf:            | Erases everything in controller cf:    |
| flash:         | Erases everything in controller flash: |
| nvram:         | Erases everything in controller nvram: |
| startup-config | Erases everything in controller usb2:  |
| usb1:          | Erases everything in controller usb1:  |

### Example

```
RFCcontroller#erase startup-config  
Erase startup-config? (y/n): n  
RFCcontroller#
```



## exit

### *Privileged Exec Mode Commands*

Ends the current CLI session and closes the session window.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
exit
```

### **Parameters**

None

### **Example**

```
RFController#exit ?
```

### format

#### *Privileged Exec Mode Commands*

Formats file system

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
format cf:
```

#### Parameters

---

|     |                       |
|-----|-----------------------|
| cf: | Formats compact flash |
|-----|-----------------------|

---

#### Example

```
RFController#format cf:  
Warning: This will destroy the contents of compact flash.  
Do you want to continue [y/n]? n  
RFController#
```

## halt

### *Privileged Exec Mode Commands*

Stops (halts) the Controller

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
halt {on <DEVICE-NAME>}
```

### Parameters

- 
- |                    |                                         |
|--------------------|-----------------------------------------|
| {on <DEVICE-NAME>} | • on – On AP/Controller                 |
|                    | • <DEVICE-NAME> – On AP/Controller name |
- 

### Example

```
RFController#halt on RFController  
RFController#
```

## help

### Privileged Exec Mode Commands

Describes the interactive help system.

Use this command to access the advanced help feature. Use “?” anytime at the command prompt to access the help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
help {show configuration-tree/search}
help search <WORD> {detailed/only-show/skip-show}
```

### Parameters

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show configuration-tree                         | <p>Displays running system information</p> <ul style="list-style-type: none"> <li>• configuration-tree – Displays the relationships among configuration objects, laid out as a tree</li> </ul>                                                                                                                                                                                                                                                                                                                                           |
| search <WORD><br>{detailed only-show skip-show} | <p>Looks for CLI commands related to a specific term</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter a term to search CLI commands for (Eg: a feature or a configuration parameter)               <ul style="list-style-type: none"> <li>• detailed – Searches and displays help strings in addition to mode and commands</li> <li>• only-show – Displays only "show" commands, not the configuration commands</li> <li>• skip-show – Displays only configuration commands, not "show" commands</li> </ul> </li> </ul> |

### Example

```
RFController#help search crypto detailed
Found 29 references for "crypto"

Mode      : Priv Exec
Command   : show crypto key rsa (|public-key-detail) (|(on
DEVICE-OR-DOMAIN-NAME))
          \ Show running system information
          \ Encryption related commands
          \ Key management operations
          \ Show RSA public Keys
```

```

\ Show the public key in PEM format
\ On AP/Controller or RF-Domain
\ AP / Controller / RF-Domain name

: show crypto pki trustpoints (WORD|all|)(|(on DEVICE-OR-DOMAIN-NAME))
\ Show running system information
\ Encryption related commands
\ Public Key Infrastructure related commands
\ Display the configured trustpoints
\ Display a particular trustpoint's details
\ Display details for all trustpoints
\ On AP/Controller or RF-Domain
\ AP / Controller / RF-Domain name

: show crypto isakmp sa (|(on DEVICE-NAME))
\ Show running system information
\ Encryption Module
\ Show ISAKMP related statistics
\ Show all ISAKMP Security Associations
\ On AP/Controller
\ AP / Controller name

: show crypto ipsec sa (|(on DEVICE-NAME))
\ Show running system information
\ Encryption Module
\ Show IPSec related statistics
\ IPSec security association
\ On AP/Controller
\ AP / Controller name

: clear crypto isakmp sa (A.B.C.D|all) (|(on DEVICE-NAME))
\ Clear
\ Encryption Module
\ ISAKMP database
\ Flush ISAKMP SAs
\ Fluch ISAKMP SAs for a given peer
.....
.....RFCont
roller>

RFController#help show configuration-tree

## ACCESS-POINT / Controller ## ---+
|
+--> [[ RF-DOMAIN ]]
|
+--> [[ PROFILE ]]
|
+--> Device specific parameters (license, serial
number, hostname)
|
+--> Configuration Overrides of rf-domain and
profile

## RF-DOMAIN ## ---+
|
+--> RF parameters, WIPS server parameters
|
+--> [[ SMART-RF-POLICY ]]
|

```

## 4 Privileged Exec Mode Commands

```

+--> [[ WIPS POLICY ]]

## PROFILE ## ---+
|
+--> Physical interface (interface GE,ME,UP etc)
|
|                                     +--> [[ RATE-LIMIT-TRUST-POLICY ]]
|
+--> Vlan interface (interface VLAN1/VLAN36 etc)
|
+--> Radio interface (interface RADIO1, RADIO2 etc)
|
|                                     +--> Radio specific Configuration
|
|                                     +--> [[ RADIO-QOS-POLICY ]]
|
|                                     +--> [[ ASSOC-ACL-POLICY ]]
|
|                                     +--> [[ WLAN ]]
|
+--> [[ MANAGEMENT-POLICY ]]
|
+--> [[ DHCP-SERVER-POLICY ]]
|
+--> [[ FIREWALL-POLICY ]]
|
+--> [[ NAT-POLICY ]]

.....
.....RFCont
roller>

RFController#help search service skip-show
Found 32 references for "service"

Mode      : Priv Exec
Command   : service show cli
           : service show rim config (|include-factory)
           : service show wireless credential-cache
           : service show wireless neighbors
           : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
           : service show process(|(on DEVICE-OR-DOMAIN-NAME))
           : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
           : service show top(|(on DEVICE-OR-DOMAIN-NAME))
           : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))
           : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
           : service cli-tables-expand (|left|right)
           : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
           : service wireless qos delete-tspeg AA-BB-CC-DD-EE-FF tid <0-7>
           : service wireless wips clear-event-history
           : service wireless wips clear-mu-blacklist (all|(mac
AA-BB-CC-DD-EE-FF))
           : service radio <1-3> dfs simulate-radar (primary|extension)
           : service smart-rf run-calibration
           : service smart-rf stop-calibration
           : service cluster manual-revert
           : service advanced-wips clear-event-history

```

```

: service advanced-wips clear-event-history
(dos-eap-failure-spoof|id-theft-out-of-sequence|id-theft-eapol-success-spoof-
detected|wlan-jack-attack-detected|essid-jack-attack-detected|monkey-jack-att
ack-detected|null-probe-response-detected|fata-jack-detected|fake-dhcp-server
-detected|crackable-wep-iv-used|windows-zero-config-memory-leak|multicast-all
-systems-on-subnet|multicast-all-routers-on-subnet|multicast-ospf-all-routers
-detection|multicast-ospf-designated-routers-detection|multicast-rip2-routers
-detection|multicast-igmp-routers-detection|multicast-vrrp-agent|multicast-hs
rp-agent|multicast-dhcp-server-relay-agent|multicast-igmp-detection|netbios-d
etection|stp-detection|ipx-detection|invalid-management-frame|invalid-channel
-advertized|dos-deauthentication-detection|dos-disassociation-detection|dos-r
ts-flood|rogue-ap-detection|accidental-association|probe-response-flood|dos-c
ts-flood|dos-eapol-logoff-storm|unauthorized-bridge)
: service start-shell
: service pktcap on(bridge|drop|deny|router|wireless|vpn|radio
(all|<1-3>) (|promiscuous)|rim|interface `WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>')(|{direction (any|inbound|outbound)|acl-name WORD|verbose|hex|count
<1-1000000>|snap <1-2048>|write (FILE|URL|tzsp WORD)|tcpdump}) (|filter LINE)

```

```

Mode      : Profile Mode
Command   : service watchdog

```

```

Mode      : Radio Mode
Command   : service antenna-type
(default|dual-band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|br
650-int)
: service disable-erp
: service disable-ht-protection
: service recalibration-interval <0-65535>
.....RFC
ontroller>

```

```

RFController>help search mint only-show
Found 8 references for "mint"

```

```

Mode      : User Exec
Command   : show mint neighbors (|details)(|(on DEVICE-NAME))
: show mint links (|details)(|(on DEVICE-NAME))
: show mint id(|(on DEVICE-NAME))
: show mint stats(|(on DEVICE-NAME))
: show mint route(|(on DEVICE-NAME))
: show mint lsp
: show mint lsp-db (|details)(|(on DEVICE-NAME))
: show mint mlcp(|(on DEVICE-NAME))
RFController>

```

## logging

### *Privileged Exec Mode Commands*

Modifies message logging facilities.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
logging monitor {<0-7>|alerts|critical|debugging|  
emergencies|errors|informational|notifications|warnings}
```

### Parameters

---

|                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| monitor<br>{<0-7> alerts critical debugging <br>emergencies errors <br>informational notifications war<br>nings} | <ul style="list-style-type: none"><li>• monitor – Sets the terminal lines logging level<ul style="list-style-type: none"><li>• &lt;0-7&gt; – Enter the logging severity level from 0-7</li><li>• alerts – Immediate action needed (severity=1)</li><li>• critical – Critical conditions (severity=2)</li><li>• debugging – Debugging messages (severity=7)</li><li>• emergencies – System is unusable (severity=0)</li><li>• errors – Error conditions (severity=3)</li><li>• informational – Informational messages (severity=6)</li><li>• notifications – Normal but significant conditions (severity=5)</li><li>• warnings – Warning conditions (severity=4)</li></ul></li></ul> |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController>logging monitor 2  
RFController>
```



## mkdir

### *Privileged Exec Mode Commands*

Creates a new directory in the filesystem

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
mkdir <DIR>
```

### **Parameters**

---

|       |                |
|-------|----------------|
| <DIR> | Directory name |
|-------|----------------|

---

### **Example**

```
RFController#mkdir testdir  
RFController#
```

## mint

### Privileged Exec Mode Commands

Configures MiNT protocol

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mint [ping|traceroute]
mint ping MINT-ID {count <1-60>|size <1-64000>|timeout <1-10>}
mint traceroute MINT-ID {destination-port <1-65535>|max-hops <1-255>|
source-port <1-65535>|timeout <1-255>}
```

### Parameters

|                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>ping MINT-ID { count &lt;1-60&gt;  size &lt;1-64000&gt;  timeout &lt;1-10&gt;}</pre>                                                     | <p>Sends a MiNT echo message to a MiNT destination</p> <ul style="list-style-type: none"> <li>• MINT-ID – Enter the MiNT destination ID to ping <ul style="list-style-type: none"> <li>• count &lt;1-60&gt; – Enter the number of times to ping from 1-60. The default value is 3</li> <li>• size &lt;1-64000&gt; – Enter the size of the MiNT payload in bytes from 1-64000. The default value is 64</li> <li>• timeout &lt;1-10&gt; – Enter the time for a response after sending a ping request from 1-10 seconds. The default timeout is 1 second</li> </ul> </li> </ul>                                                                       |
| <pre>traceroute MINT-ID { destination-port &lt;1-65535&gt;  max-hops &lt;1-255&gt;  source-port &lt;1-65535&gt;  timeout &lt;1-255&gt;}</pre> | <p>Print the route packets trace to a device</p> <ul style="list-style-type: none"> <li>• MINT-ID – Enter the MiNT destination id <ul style="list-style-type: none"> <li>• destination-port &lt;1-65535&gt; – Enter the destination port value to be used for ECMP (default 45)</li> <li>• max-hops &lt;1-255&gt; – Enter the maximum number of hops, a traceroute packet traverses in forward direction.(default 30)</li> <li>• source-port &lt;1-65535&gt; – Enter the source port value to be used for ECMP (default 45)</li> <li>• timeout &lt;1-65535&gt; – Enter the time to wait for a response (default 30 seconds)</li> </ul> </li> </ul> |

### Example

```
RFCcontroller>mint ping 70.37.FA.BF count 20 size 128
MiNT ping 70.37.FA.BF with 128 bytes of data.
Response from 70.37.FA.BF: id=1 time=0.292 ms
Response from 70.37.FA.BF: id=2 time=0.206 ms
Response from 70.37.FA.BF: id=3 time=0.184 ms
Response from 70.37.FA.BF: id=4 time=0.160 ms
Response from 70.37.FA.BF: id=5 time=0.138 ms
Response from 70.37.FA.BF: id=6 time=0.161 ms
Response from 70.37.FA.BF: id=7 time=0.174 ms
Response from 70.37.FA.BF: id=8 time=0.207 ms
```

```
Response from 70.37.FA.BF: id=9 time=0.157 ms
Response from 70.37.FA.BF: id=10 time=0.153 ms
Response from 70.37.FA.BF: id=11 time=0.159 ms
Response from 70.37.FA.BF: id=12 time=0.173 ms
Response from 70.37.FA.BF: id=13 time=0.156 ms
Response from 70.37.FA.BF: id=14 time=0.209 ms
Response from 70.37.FA.BF: id=15 time=0.147 ms
Response from 70.37.FA.BF: id=16 time=0.203 ms
Response from 70.37.FA.BF: id=17 time=0.148 ms
Response from 70.37.FA.BF: id=18 time=0.169 ms
Response from 70.37.FA.BF: id=19 time=0.164 ms
Response from 70.37.FA.BF: id=20 time=0.177 ms
```

```
--- 70.37.FA.BF ping statistics ---
```

```
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 0.138/0.177/0.292 ms
```

### more

#### *Privileged Exec Mode Commands*

Displays the contents of a file

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
more <FILE>
```

#### Parameters

---

|        |                                   |
|--------|-----------------------------------|
| <FILE> | Displays the contents of the file |
|--------|-----------------------------------|

---

#### Example

```
RFController#more flash:/log/messages.log
May 03 11:45:05 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/dpd2"
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioc1.c:335 dev_dataplane_fw_ioc1 DHCP
trust of port 0 (ge1) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioc1.c:335 dev_dataplane_fw_ioc1 DHCP
trust of port 1 (ge2) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioc1.c:335 dev_dataplane_fw_ioc1 DHCP
trust of port 2 (ge3) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %KERN-6-INFO: 0| ioc1.c:335 dev_dataplane_fw_ioc1 DHCP
trust of port 3 (ge4) set to 1 by 1021 cfgd.
May 03 11:45:14 2010: %NSM-4-IFDOWN: Interface vlan1 is down
May 03 11:45:14 2010: %NSM-4-IFUP: Interface vlan4 is up
May 03 11:45:15 2010: %NSM-4-IFUP: Interface vlan44 is up
May 03 11:45:15 2010: %NSM-4-IFDOWN: Interface vlan44 is down
May 03 11:45:15 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/lighttpd"
May 03 11:45:15 2010: %FILEMGMT-5-HTTPSTART: lighttpd started in external mode
with pid 0
May 03 11:45:15 2010: %USER-5-NOTICE: FILEMGMT[1064]: FTP: ftp server stopped
May 03 11:45:15 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/telnetd"
May 03 11:45:17 2010: %AUTH-6-INFO: sshd[1371]: Server listening on 0.0.0.0
port 22.
May 03 11:45:17 2010: %AUTOINSTD-5-AUTOCLCONFDISAB: Autoinstall of cluster
configuration is disabled
May 03 11:45:17 2010: %AUTOINSTD-5-AUTOCONFDISAB: Autoinstall of startup
configuration is disabled
May 03 11:45:17 2010: %AUTOINSTD-5-AUTOIMAGEDISAB: Autoinstall of image
upgrade is disabled
May 03 11:45:18 2010: %KERN-6-INFO: dataplane enabled.
RFController#
```

## no

### *Privileged Exec Mode Commands*

Use the no command to revert a command or to set parameters to their default values. This command is useful if you would like to turn off an enabled feature or set default values for a parameter

---

#### **NOTE**

The commands have their own set of parameters that can be reset.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
no
[adoption|captive-portal|crypto|debug|logging|page|service|terminal|upgrade|
wireless]
```

#### **Parameters**

None

#### **Usage Guidelines**

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

#### **Example**

```
RFController>no adoption
RFController>

RFController>no page
RFController>

RFController>no service cli-tables-expand line
RFController>
```

### page

#### *Privileged Exec Mode Commands*

Use the command to toggle the Controller paging function. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
page
```

#### **Parameters**

None

#### **Example**

```
RFController#page  
RFController#
```

## ping

### *Privileged Exec Mode Commands*

Sends ICMP echo messages to a user-specified location

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ping { [<IP>|<hostname> ] }
```

### Parameters

---

|                             |                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ping { [<IP> <hostname> ] } | Pings the specified destination IP address or hostname. When entered without any parameters, this command prompts for an IP/Host-name to ping. |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController#ping 172.16.10.3
PING 172.16.10.3 (172.16.10.3): 100 data bytes
108 bytes from 172.16.10.3: seq=0 ttl=64 time=7.100 ms
108 bytes from 172.16.10.3: seq=1 ttl=64 time=0.390 ms
108 bytes from 172.16.10.3: seq=2 ttl=64 time=0.422 ms
108 bytes from 172.16.10.3: seq=3 ttl=64 time=0.400 ms

--- 172.16.10.3 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.390/2.078/7.100 ms
RFController#
```

### pwd

#### *Privileged Exec Mode Commands*

View the contents of the current directory

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
pwd
```

#### **Parameters**

None

#### **Example**

```
RFController#pwd  
flash:/  
RFController#
```



## reload

### *Privileged Exec Mode Commands*

Halts the Controller and performs a warm reboot

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
reload {force {on|<DEVICE-OR-DOMAIN-NAME>}|on <DEVICE-OR-DOMAIN-NAME>}
```

### Parameters

---

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{force<br/>{on &lt;DEVICE-OR-DOMAIN-NAM<br/>E&gt;} on<br/>&lt;DEVICE-OR-DOMAIN-NAME&gt;}</pre> | <ul style="list-style-type: none"> <li>• force {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Forces reboot ignoring conditions like upgrade in progress, unsaved changes etc             <ul style="list-style-type: none"> <li>• on – On AP/Controller or RF-Domain                 <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF-Domain name</li> </ul> </li> </ul> </li> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – On AP/Controller or RF-Domain             <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF-Domain name</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController#reload force on RFController
RFController#
```

### rename

#### *Privileged Exec Mode Commands*

Renames a file in the existing filesystem

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
rename <FILE> <FILE>
```

#### **Parameters**

---

|               |                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| <FILE> <FILE> | Specifies the file to rename. The first <FILE> is the old file name. The second <FILE> defines the new file name. |
|---------------|-------------------------------------------------------------------------------------------------------------------|

---

#### **Example**

```
RFController#rename flash:/testdir/ testdir1
RFController#
```

## revert

### *Privileged Exec Mode Commands*

Reverts the changes made in the active session to their last saved configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
revert
```

### **Parameters**

None

### **Example**

```
RFController#revert  
RFController#
```

### rmdir

#### *Privileged Exec Mode Commands*

Deletes an existing file from the filesystem

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
rmdir <DIR>
```

#### **Parameters**

---

|       |                                             |
|-------|---------------------------------------------|
| <DIR> | Defines the name of the directory to delete |
|-------|---------------------------------------------|

---

#### **Example**

```
RFController#rmdir flash:/testdir1  
RFController#
```

## self

### *Privileged Exec Mode Commands*

Displays the configuration context of the currently logged device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
self
```

### **Parameters**

None

### **Example**

```
RFController#self
Enter configuration commands, one per line. End with CNTL/Z.
RFController(config-device-00-15-70-37-FA-BE)#
```

### service

#### *Privileged Exec Mode Commands*

The service command performs different functions depending on the parameter passed to it. Generally, this command is used to directly interact with the device to force an action on the device.

---

**NOTE**

Service commands have their own set of parameters. Please refer to the [Chapter 6, service](#) for a list of parameters used with the service command.

---

**Syntax**

```
service
[advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster|copy|force-sen
d-config|locator|mint|noc|pktcap|pm|radio|radius|set|show|smart-rf|start-shel
l|wireless|signal
```

**Parameters**

---

**NOTE**

Please see [Chapter 6, service](#) for more information.

---

**Example**

```
RFController#service start-shell
Last password used: tddxjoht with MAC 00:15:70:37:fa:be
Password:

RFController#service wireless client beacon-request 11-22-33-44-55-66 mode act
ive ssid test channel-report none
```

## show

### *Privileged Exec Mode Commands*

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances
- When invoked with the display\_parameter, it displays information about that component.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show <parameter>
```

### Parameters

---

### NOTE

Refer to '[Chapter 7, Show Commands](#)' for more information.

---

### Example

```
RFController#show ?
  adoption          Display information related to adoption to wireless
                    controller
  advanced-wips     Advanced WIPS
  ap-upgrade        AP Upgrade
  boot              Display boot configuration.
  captive-portal    Captive portal commands
  cdp               Cisco Discovery Protocol
  clock             Display system clock
  cluster           Cluster Protocol
  commands          Show command lists
  context           Information about current context
  critical-resources Critical Resources
  crypto            Encryption related commands
  debug            Debugging functions
  debugging         Debugging functions
  device-categorization Device Categorization
  event-history     Display event history
  event-system-policy Display event system policy
  file             Display filesystem information
  firewall          Wireless Firewall
  interface         Interface Configuration/Statistics commands
  ip               Internet Protocol (IP)
```

## 4 Privileged Exec Mode Commands

|                       |                                            |
|-----------------------|--------------------------------------------|
| ip-access-list-stats  | IP Access list stats                       |
| licenses              | Show installed licenses and usage          |
| lldp                  | Link Layer Discovery Protocol              |
| logging               | Show logging information                   |
| mac-access-list-stats | MAC Access list stats                      |
| mac-address-table     | Display MAC address table                  |
| mint                  | MiNT protocol                              |
| noc                   | Noc-level information                      |
| ntp                   | Network time protocol                      |
| password-encryption   | Pasword encryption                         |
| power                 | Show power over ethernet command           |
| remote-debug          | Show details of remote debug sessions      |
| rf-domain-manager     | Show RF Domain Manager selection details   |
| role                  | Role based firewall                        |
| running-config        | Current operating configuration            |
| session-changes       | Configuration changes made in this session |
| session-config        | This session configuration                 |
| sessions              | Display CLI sessions                       |
| smart-rf              | Smart-RF Management Commands               |
| spanning-tree         | Display spanning tree information          |
| startup-config        | Startup configuration                      |
| terminal              | Display terminal configuration parameters  |
| timezone              | The timezone                               |
| upgrade-status        | Display last image upgrade status          |
| version               | Display software & hardware version        |
| wireless              | Wireless commands                          |
| wwan                  | Display wireless WAN Status                |



## telnet

### *Privileged Exec Mode Commands*

Opens a telnet session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
telnet <IP> {port}
```

### Parameters

---

|             |                                                                                    |
|-------------|------------------------------------------------------------------------------------|
| <IP> {port} | Defines an IP address or hostname of a remote system                               |
|             | <ul style="list-style-type: none"><li>• port – Enter the TCP port number</li></ul> |

---

### Example

```
RFController#telnet 172.16.10.1

Entering character mode
Escape character is '^]'.
RFS7000 release 5.1.0.0
RFController login: cli
NOTE: logging in as 'cli' w/o password is going away. Use admin accounts under
management-policy [Eg: admin/admin123]
Welcome to CLI
RFController>
```

## terminal

### *Privileged Exec Mode Commands*

Sets the length/number of lines displayed within the terminal window

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
terminal [length|width] <0-512>
```

### Parameters

|                |                                                        |
|----------------|--------------------------------------------------------|
| length <0-512> | Sets the number of lines on a screen                   |
| width <0-512>  | Sets the width/number of characters on the screen line |

### Example

```
RFController#terminal length 150
RFController#

RFController#terminal width 215
RFController#
```

## time-it

### *Privileged Exec Mode Commands*

Verifies the time taken by a particular command between request and response

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
time-it <LINE>
```

### Parameters

---

|        |                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------|
| <LINE> | Verifies the time taken by a particular command between request and response                              |
|        | <ul style="list-style-type: none"><li>• &lt;LINE&gt; - Specify the command to view the response</li></ul> |

---

### Example

```
RFController#time-it enable
That took 0.00 seconds..
RFController#
```

### traceroute

#### *Privileged Exec Mode Commands*

Traces the route to a defined destination.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
traceroute <LINE>
```

#### **Parameters**

---

|        |                                                          |
|--------|----------------------------------------------------------|
| <LINE> | Traces the route to a destination IP address or hostname |
|--------|----------------------------------------------------------|

---

#### **Example**

```
RFController#traceroute 172.16.10.2
traceroute to 172.16.10.2 (172.16.10.2), 30 hops max, 38 byte packets
 1 172.16.10.1 (172.16.10.1) 3002.008 ms !H 3002.219 ms !H 3003.945 ms !H
RFController>
```

## upgrade

### *Privileged Exec Mode Commands*

Upgrades the software image

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
upgrade <URL> {background|on <DEVICE-NAME>}
```

### Parameters

|                  |                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <URL>            | Sets the location of the target firmware image used in the upgrade                                                                  |
| background       | Optional. Specifies the upgrade should occur in the background                                                                      |
| on <DEVICE-NAME> | on <DEVICE-NAME> – On AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> |

### Example

```
RFController#upgrade tftp://157.235.208.105:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

RFController#upgrade tftp://157.125.208.235/img
Running from partition /dev/mtdblock7, partition to update is /dev/mtdblock6
```

### upgrade-abort

#### *Privileged Exec Mode Commands*

Aborts an ongoing software image upgrade

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
upgrade-abort {<on> <DEVICE-OR-DOMAIN-NAME>}
```

#### **Parameters**

---

|                         |                                                                  |
|-------------------------|------------------------------------------------------------------|
| on                      | on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF-Domain       |
| <DEVICE-OR-DOMAIN-NAME> | • <DEVICE-OR-DOMAIN-NAME> – On AP/Controller name/RF-Domain name |

---

#### **Example**

```
RFController#upgrade-abort on RFController
Error: No upgrade in progress
RFController#
```

## watch

### *Privileged Exec Mode Commands*

Repeats the specific CLI command at a periodic interval

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
watch <1-3600> <LINE>
```

### Parameters

---

|                 |                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------|
| <1-3600> <LINE> | Repeats the specified CLI command on the specified interval(s). Select an interval from 1-3600 seconds |
|-----------------|--------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController#watch 45 page
RFController#
```

## write

### *Privileged Exec Mode Commands*

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
write
```

### Parameters

|          |                     |
|----------|---------------------|
| memory   | Writes to NV memory |
| terminal | Writes to terminal  |

### Example

```
RFController#write memory
[OK]
RFController#
```

```
RFController#write terminal
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
enable
calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
voice-prioritization
svp-prioritization
wmm background cw-max 8
wmm video txop-limit 9
RFController>
```



# Global Configuration Commands

---

## In this chapter

- [Global Configuration Commands](#) ..... 136

This chapter summarizes the global-configuration commands in the CLI command structure.

The term `global` is used to indicate characteristics or features effecting the system as a whole. Use the Global Configuration Mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the `configure terminal` command (under PRIV EXEC) to enter the global configuration mode.

The example below describes the process of entering the global configuration mode from the privileged EXEC mode:

```
RFController# configure terminal
RFController(config)#
```

---

**NOTE**

The system prompt changes to indicate you are now in the global configuration mode. The prompt consists of the device host name followed by `(config)` and a pound sign (`#`).

---

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a `copy running-config startup-config` EXEC command is issued.

## Global Configuration Commands

Table 5 Summarizes global configuration commands

**TABLE 5** Global Configuration Commands

| Command                                  | Description                                                                | Reference                |
|------------------------------------------|----------------------------------------------------------------------------|--------------------------|
| <a href="#">aaa-policy</a>               | Configures an aaa-policy                                                   | <a href="#">page 138</a> |
| <a href="#">advanced-wips-policy</a>     | Configures an advanced-wips-policy                                         | <a href="#">page 139</a> |
| <a href="#">association-acl-policy</a>   | Configures an association-acl-policy                                       | <a href="#">page 140</a> |
| <a href="#">auto-provisioning-policy</a> | Configures an auto-provisioning-policy                                     | <a href="#">page 141</a> |
| <a href="#">br650</a>                    | Adds a Mobility 650 Access Point to the controller managed network         | <a href="#">page 142</a> |
| <a href="#">br6511</a>                   | Adds a Mobility 6511 Access Point to the controller managed network        | <a href="#">page 143</a> |
| <a href="#">br6532</a>                   | Adds a Mobility 6532 Access Point to the controller managed network        | <a href="#">page 144</a> |
| <a href="#">br71xx</a>                   | Adds a Mobility 7131 Series Access Point to the controller managed network | <a href="#">page 145</a> |
| <a href="#">captive-portal</a>           | Configures a captive portal                                                | <a href="#">page 147</a> |
| <a href="#">clear</a>                    | Clears the event history                                                   | <a href="#">page 162</a> |
| <a href="#">critical-resource-policy</a> | Configures critical-resource-policy settings                               | <a href="#">page 164</a> |
| <a href="#">customize</a>                | Customizes the output of summary cli commands                              | <a href="#">page 168</a> |
| <a href="#">device</a>                   | Specifies configuration on multiple devices                                | <a href="#">page 172</a> |
| <a href="#">device-categorization</a>    | Configures a device categorization object                                  | <a href="#">page 174</a> |
| <a href="#">dhcp-server-policy</a>       | Configures a dhcp-server-policy                                            | <a href="#">page 178</a> |
| <a href="#">dns-whitelist</a>            | Configures a whitelist                                                     | <a href="#">page 180</a> |
| <a href="#">do</a>                       | Runs commands from the EXEC mode                                           | <a href="#">page 184</a> |
| <a href="#">end</a>                      | Ends and exits the current mode and moves to the PRIV EXEC mode            | <a href="#">page 186</a> |
| <a href="#">event-system-policy</a>      | Configures an event system policy                                          | <a href="#">page 188</a> |
| <a href="#">firewall-policy</a>          | Configures a firewall-policy                                               | <a href="#">page 199</a> |
| <a href="#">help</a>                     | Displays interactive help system                                           | <a href="#">page 200</a> |
| <a href="#">host</a>                     | Sets the system's network name                                             | <a href="#">page 202</a> |
| <a href="#">igmp-snoop-policy</a>        | Configures a igmp-snoop-policy                                             | <a href="#">page 203</a> |
| <a href="#">ip</a>                       | Configures a selected <i>Internet Protocol</i> (IP) component              | <a href="#">page 204</a> |
| <a href="#">mac</a>                      | Configures MAC access lists (goes to the MAC ACL mode)                     | <a href="#">page 205</a> |
| <a href="#">management-policy</a>        | Configures a management-policy                                             | <a href="#">page 206</a> |
| <a href="#">mint-policy</a>              | Configures a mint-security-policy                                          | <a href="#">page 207</a> |
| <a href="#">nac-list</a>                 | Configures a network access control list (ACL)                             | <a href="#">page 209</a> |
| <a href="#">no</a>                       | Negates a command or sets its default values                               | <a href="#">page 214</a> |
| <a href="#">password-encryption</a>      | Enables password encryption in configuration                               | <a href="#">page 216</a> |

**TABLE 5** Global Configuration Commands

| <b>Command</b>                 | <b>Description</b>                                            | <b>Reference</b>         |
|--------------------------------|---------------------------------------------------------------|--------------------------|
| <i>profile</i>                 | Configures profile related commands                           | <a href="#">page 217</a> |
| <i>radio-qos-policy</i>        | Configures a radio-qos-policy                                 | <a href="#">page 219</a> |
| <i>radius-group</i>            | Configures a radius-group                                     | <a href="#">page 220</a> |
| <i>radius-server-policy</i>    | Configures a radius-server-policy                             | <a href="#">page 221</a> |
| <i>radius-user-pool-policy</i> | Configures a radius-user-pool-policy                          | <a href="#">page 222</a> |
| <i>rf-domain</i>               | Creates a RF-Domain                                           | <a href="#">page 224</a> |
| <i>rfs4000</i>                 | Adds a Mobility RFS4000 Controller to the network             | <a href="#">page 229</a> |
| <i>rfs6000</i>                 | Adds a Mobility RFS6000 Controller to the network             | <a href="#">page 230</a> |
| <i>rfs7000</i>                 | Adds a Mobility RFS7000 Controller to the network             | <a href="#">page 231</a> |
| <i>role-policy</i>             | Configures a role-policy                                      | <a href="#">page 232</a> |
| <i>self</i>                    | Displays the configuration context of the logged device       | <a href="#">page 233</a> |
| <i>service</i>                 | Retrieves system data                                         | <a href="#">page 234</a> |
| <i>show</i>                    | Displays running system information                           | <a href="#">page 236</a> |
| <i>smart-rf-policy</i>         | Configures a Smart-RF-policy                                  | <a href="#">page 238</a> |
| <i>wips-policy</i>             | Configures a wips-policy                                      | <a href="#">page 239</a> |
| <i>wlan</i>                    | Configures a wireless WLAN                                    | <a href="#">page 241</a> |
| <i>wlan-qos-policy</i>         | Configures a WLAN-QoS-policy                                  | <a href="#">page 282</a> |
| <i>write</i>                   | Writes the system running configuration to memory or terminal | <a href="#">page 283</a> |

## aaa-policy

### *Global Configuration Commands*

Configures an authentication/accounting/authorization policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
aaa-policy <aaa-policy-name>
```

### **Parameters**

---

|                   |                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------|
| <aaa-policy-name> | Defines the name of the aaa-policy to be configured (will be created if it does not exist) |
|-------------------|--------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config)#aaa-policy test
RFController(config-aaa-policy test)#
```

### **NOTE**

For more information, see [Chapter 9, aaa-policy](#).

---

## advanced-wips-policy

### *Global Configuration Commands*

Configures an advanced-wips-policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
advanced-wips-policy <advanced-wips-policy-name>
```

### **Parameters**

---

|                             |                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------|
| <advanced-wips-policy-name> | Sets the name of the advanced-wips policy (will be created if it does not already exist) |
|-----------------------------|------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config)#advanced-wips-policy test
RFController(config)#
```

### **NOTE**

For more information, see [Chapter 7, Show Commands](#).

---

## association-acl-policy

### *Global Configuration Commands*

Configures an association-acl-policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
association-acl-policy <association-acl-policy-name>
```

### **Parameters**

---

|                               |                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------|
| <association-acl-policy-name> | Enter the name of the association-acl-policy (will be created if it does not already exist) |
|-------------------------------|---------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config)#association-acl-policy test
RFController(config)#
```

### **NOTE**

For more information, see [Chapter 12, association-acl-policy](#).

---

## auto-provisioning-policy

### *Global Configuration Commands*

Configures an auto-provisioning policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
auto-provisioning-policy <AUTO-PROVISIONING-POLICY>
```

### **Parameters**

---

|                            |                                                       |
|----------------------------|-------------------------------------------------------|
| <AUTO-PROVISIONING-POLICY> | Name of the auto-provisioning policy to be configured |
|----------------------------|-------------------------------------------------------|

---

### **Example**

```
RFController(config)#auto-provisioning-policy test
RFController(config-auto-provisioning-policy-test)#
```

---

### **NOTE**

For more information see [Chapter 10, auto-provisioning-policy](#)

---

## br650

### Global Configuration Commands

Adds a Mobility 650 Access Point to the controller managed network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
br650 <MAC>
```

### Parameters

---

|                          |                                                               |
|--------------------------|---------------------------------------------------------------|
| <code>&lt;MAC&gt;</code> | Enter the MAC address of the target Mobility 650 Access Point |
|--------------------------|---------------------------------------------------------------|

---

### Example

```
RFController(config)#br650 11-22-33-44-55-66 ?
RFController(config-device-11-22-33-44-55-66)
```

```
RFController(config)#show wireless ap configured
```

| IDX | NAME          | MAC               | PROFILE        | RF-DOMAIN |
|-----|---------------|-------------------|----------------|-----------|
| 1   | br7131-889EC4 | 00-15-70-88-9E-C4 | default-br7131 | default   |
| 2   | br650-445566  | 11-22-33-44-55-66 | default-br650  | default   |

```
RFController(config)#
```



## br6511

### *Global Configuration Commands*

Adds a Mobility 6511 Access Point to the controller managed network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
br6511 <MAC>
```

### **Parameters**

---

|       |                                                                |
|-------|----------------------------------------------------------------|
| <MAC> | Enter the MAC address of the target Mobility 6511 Access Point |
|-------|----------------------------------------------------------------|

---

### **Example**

```
RFController(config)#br6511 00-17-70-88-9E-C4 ?  
RFController(config-device-00-17-70-88-9E-C4)#
```

## br6532

### *Global Configuration Commands*

Adds a Mobility 6532 Access Point to the controller managed network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
br6532 <MAC>
```

### **Parameters**

---

|       |                                                                |
|-------|----------------------------------------------------------------|
| <MAC> | Enter the MAC address of the target Mobility 6532 Access Point |
|-------|----------------------------------------------------------------|

---

### **Example**

```
RFController(config)#br6532 00-27-70-89-9F-E4 ?  
RFController(config-device-00-27-70-89-9F-E4)#
```

## br71xx

### *Global Configuration Commands*

Adds a Mobility 7131 Series Access Point to the controller managed network using its MAC address. If a profile for the AP is not available, a new profile is created.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
br71xx <MAC>
```

### **Parameters**

---

|       |                                                                       |
|-------|-----------------------------------------------------------------------|
| <MAC> | Enter the MAC address of the target Mobility 7131 Series Access Point |
|-------|-----------------------------------------------------------------------|

---

### **Example**

```
RFController(config)#br71xx 00-15-70-88-9E-C4 ?  
RFController(config-device-00-15-70-88-9E-C4)#
```

## Captive Portal Mode

### [Global Configuration Commands](#)

The Captive Portal Mode provides the commands to configure a hotspot. The following table lists the command to enter the Captive Portal configuration mode.

| Command                        | Description                                   | Reference                |
|--------------------------------|-----------------------------------------------|--------------------------|
| <a href="#">captive-portal</a> | Configures captive portal Web page parameters | <a href="#">page 147</a> |

## captive-portal

### *Global Configuration Commands*

Configures a captive portal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
captive-portal <CAPTIVE-PORTAL>
```

### **Parameters**

---

|                  |                                                                                              |
|------------------|----------------------------------------------------------------------------------------------|
| <CAPTIVE-PORTAL> | Enter the name of the captive portal being configured (will be created if it does not exist) |
|------------------|----------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config)#captive-portal testportal  
RFController(config-captive-portal-testportal)#
```

## Captive-Portal-Mode Commands

Table 6 Summarizes captive-portal mode commands

**TABLE 6** captive-portal-mode Commands

| Command                            | Description                                                                                             | Reference                |
|------------------------------------|---------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">access-time</a>        | Defines allowed access time for a client. It is used when no session time is defined in RADIUS response | <a href="#">page 149</a> |
| <a href="#">access-type</a>        | Configures the access type for a captive portal from the list                                           | <a href="#">page 150</a> |
| <a href="#">accounting</a>         | Enables accounting records for a captive portal                                                         | <a href="#">page 151</a> |
| <a href="#">connection-mode</a>    | Configures the connection mode for a captive portal                                                     | <a href="#">page 152</a> |
| <a href="#">custom-auth</a>        | Configures custom user information                                                                      | <a href="#">page 153</a> |
| <a href="#">inactivity-timeout</a> | Defines an inactivity timeout in seconds                                                                | <a href="#">page 154</a> |
| <a href="#">server</a>             | Configures the captive portal server's configuration                                                    | <a href="#">page 155</a> |
| <a href="#">simultaneous-users</a> | Specifies a particular user name that can only be used by a certain pool of MAC addresses at a time     | <a href="#">page 156</a> |
| <a href="#">terms-agreement</a>    | Enforces the user to agree to terms and conditions (included in login page) for captive portal access   | <a href="#">page 157</a> |
| <a href="#">use</a>                | Defines captive portal configuration settings                                                           | <a href="#">page 158</a> |
| <a href="#">webpage-location</a>   | Specifies the location of the webpages used for captive portal authentication                           | <a href="#">page 159</a> |
| <a href="#">webpage</a>            | Configures captive portal webpage parameters                                                            | <a href="#">page 160</a> |

## *access-time*

### *Captive-Portal-Mode Commands*

Defines the permitted access time for a client. It is used when no session time is defined in RADIUS response.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
access-time <30-10080>
```

### **Parameters**

---

|            |                                                                                        |
|------------|----------------------------------------------------------------------------------------|
| <30-10080> | Enter the time from <30-10080> minutes to define the allowed access time for a client. |
|------------|----------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#access-time 35  
RFController(config-captive-portal-test)#
```

## *access-type*

### *Captive-Portal-Mode Commands*

Defines the captive portal access type

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
access-type [custom-auth-radius|logging|no-auth|radius]
```

### **Parameters**

---

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [custom-auth-radius <br>logging no-auth radius] | <ul style="list-style-type: none"><li>• custom-auth-radius – Verifies custom user information for authentication (RADIUS lookup with given information. For example:- Name, E-mail Address, Telephone)</li><li>• logging – Generates a logging record of user access and allowed access</li><li>• no-auth – No authentication for a guest is required (redirected to welcome message)</li><li>• radius – Configures radius authentication</li></ul> |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#access-type radius
RFController(config-captive-portal-test)#

RFController(config-captive-portal-testportal)#access-type logging
RFController(config-captive-portal-testportal)#
```



## *accounting*

### *Captive-Portal-Mode Commands*

Enables accounting records for a captive portal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
accounting [radius|syslog]
accounting syslog host <WORD> {port} <1-65535>
```

### **Parameters**

|                                     |                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius                              | Enables support for RADIUS accounting messages                                                                                                                                                                                                                                                       |
| syslog host <WORD> {port} <1-65535> | Enables support for syslog accounting messages <ul style="list-style-type: none"> <li>• host &lt;WORD&gt; – Specify a syslog destination hostname or IP address for accounting records</li> <li>• {port} &lt;1-65535&gt; – Specify a UDP port number of syslog server between 1 and 65535</li> </ul> |

### **Example**

```
RFController(config-captive-portal-test)#accounting syslog host 172.16.10.13
port 1
RFController(config-captive-portal-test)#
```

## *connection-mode*

### *Captive-Portal-Mode Commands*

Configures the captive portal connection mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
connection-mode [http|https]
```

### **Parameters**

- 
- |              |                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------|
| [http https] | <ul style="list-style-type: none"><li>• http – Connection-mode is http</li><li>• https – Connection-mode is https</li></ul> |
|--------------|-----------------------------------------------------------------------------------------------------------------------------|
- 

### **Example**

```
RFController(config-captive-portal-test)#connection-mode https
RFController(config-captive-portal-test)#
```

## *custom-auth*

### *Captive-Portal-Mode Commands*

Configures custom user information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
custom-auth info <LINE>
```

### **Parameters**

---

|             |                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| info <LINE> | Information used for RADIUS lookup when custom-auth-radius access type is configured. <ul style="list-style-type: none"> <li>• &lt;LINE&gt; - Guest data needs to be provided. Enter the name, email address and telephone number of the user</li> </ul> |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#custom-auth info testuser
robert@brocade.com
RFController(config-captive-portal-test)#

RFController(config-captive-portal-testportal)#custom-auth info bob,
bob@brocade.com, 9902833119
RFController(config-captive-portal-testportal)#show context
captive-portal testportal
  access-type logging
  custom-auth info bob,\ bob@brocade.com,\ 9902833119
RFController(config-captive-portal-testportal)#
```

## *inactivity-timeout*

### *Captive-Portal-Mode Commands*

Defines an inactivity timeout in seconds. If a frame is not received from a client for the specified time interval, the current session is terminated

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
inactivity-timeout <300-1800>
```

### **Parameters**

---

|            |                                                                   |
|------------|-------------------------------------------------------------------|
| <300-1800> | Sets a time from 300-1800 seconds to define an inactivity timeout |
|------------|-------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#inactivity-timeout 750
RFController(config-captive-portal-test)#
```

## *server*

### *Captive-Portal-Mode Commands*

Configures captive portal server parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
server [host <WORD> | mode]
server mode [centralized | centralized-controller | self]
```

### **Parameters**

---

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [host <WORD>   mode] | <ul style="list-style-type: none"> <li>• host &lt;WORD&gt; – Configures the address of the captive portal server <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter the IP address or hostname of the internal captive portal server</li> </ul> </li> <li>• mode [centralized   centralized-controller   self] – Configures the captive portal server mode <ul style="list-style-type: none"> <li>• centralized – Considers the configured server hostname or IP address as the centralized captive portal server</li> <li>• centralized-controller – Uses the configured hostname as the virtual captive portal server name across Controllers</li> <li>• self – Selects the captive portal server as the same device supporting the WLAN</li> </ul> </li> </ul> |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#server mode self
RFController(config-captive-portal-test)#
```

```
RFController(config-captive-portal-test)#server host 172.16.10.9
RFController(config-captive-portal-test)#
```

## *simultaneous-users*

### *Captive-Portal-Mode Commands*

Specifies a particular user name that can only be used by a certain number of MAC addresses at a time

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
simultaneous-users <0-8192>
```

### **Parameters**

---

|          |                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <0-8192> | Sets the number of MAC addresses allowed to use that username at the same time. Select a number between 0 and 8192 (0 implies unlimited). |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#simultaneous-users 5  
RFController(config-captive-portal-test)#
```

## *terms-agreement*

### *Captive-Portal-Mode Commands*

Enforces the user to agree to terms and conditions (included in login page) for captive portal guest access to the controller

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
terms-agreement
```

### **Parameters**

None

### **Example**

```
RFController(config-captive-portal-test)#terms-agreement  
RFController(config-captive-portal-test)#
```

## *use*

### *Captive-Portal-Mode Commands*

Defines configuration settings for the captive portal configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
use [aaa-policy <aaa-policy-name>|dns-whitelist <dns-whitelist>]
```

### **Parameters**

---

```
[aaa-policy  
<aaa-policy-name>|  
dns-whitelist  
<dns-whitelist-policy>]
```

- `aaa-policy <aaa-policy-name>` – Configures a aaa-policy for the captive portal
    - `<aaa-policy-name>` – Enter a policy name for authenticating captive portal users
  - `dns-whitelist <dns-whitelist-policy>` – Configures a DNS whitelist for the captive portal
    - `<dns-whitelist>` – Enter a DNS whitelist to configure
- 

### **Example**

```
RFController(config-captive-portal-test)#use aaa-policy test  
RFController(config-captive-portal-test)#
```



## *webpage-location*

### *Captive-Portal-Mode Commands*

Specifies the location of the Webpages used for authentication. These pages can either be hosted on the system or an external Web server

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
webpage-location [advanced|external|internal]
```

### **Parameters**

---

|                              |                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [advanced external internal] | <ul style="list-style-type: none"><li>• advanced – Uses login/welcome/failure Web pages created by the user on the system</li><li>• external – Uses login/welcome/failure Web pages on an external server (External URL required)</li><li>• internal – Uses login/welcome/failure Web pages created automatically on the system</li></ul> |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-captive-portal-test)#webpage-location internal
RFController(config-captive-portal-test)#

RFController(config-captive-portal-test)#webpage internal agreement title
test123
RFController(config-captive-portal-test)#
```

### *webpage*

#### *Captive-Portal-Mode Commands*

Configures captive portal Web page parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
webpage [external|internal]
webpage external [fail|login|welcome] <URL>
webpage internal [agreement|fail|login|welcome]
webpage internal [agreement|fail|login|welcome]
[description|footer|header|main-logo|small-logo|title]
webpage internal [agreement|fail|login|welcome]
[description|footer|header|title] <LINE>
webpage internal [agreement|fail|login|welcome] [main-logo|small-logo] <WORD>
```

## Parameters

external [fail|login|welcome ]  
<URL>]

Configures captive portal external page links

- fail <URL> – Users are redirected to this Webpage if they fail authentication
- login <URL> – Users are prompted for their username and password on this Webpage
- welcome <URL> – Users are redirected to this Webpage after they authenticate successfully

The following parameter is common for the above:

- <URL> – Enter the URL used for remote captive portal staging. The length can be to 1024 characters

internal [agreement|fail|login|  
welcome]  
[description|footer|header|  
main-logo|small-logo|title]

Configures captive portal internal page parameters

- agreement – Users are prompted to agree the terms in this page when terms-agreement is enabled
- fail – Users are redirected to this Webpage if they fail authentication
- login – Users are prompted for their username and password on this Webpage
- welcome – Users are redirected to this Webpage after they authenticate successfully

The following parameters are common for the above:

- description <LINE> – Text displayed as the main body (normal font, middle of page) of the Webpage
- footer <LINE> – Text displayed at the footer (smaller font, bottom section) of the Webpage
- header <LINE> – Text displayed as a header (large font, top section) of the Webpage
- title <LINE> – Text that will be the title of the Webpage

The following parameter is common for the above:

- <LINE> – Enter a string value. The length can be to 1024 characters
- main-logo <WORD> – Main image (large size) displayed by the local Webpage. Appears between the header and description on the Webpage
- small-logo <WORD> – Small image (thumbnail size) displayed by the local webpage. Appears near the footer on the Webpage

The following parameter is common for the above:

- <WORD> – Enter the URL from where the image is loaded and cached to the system

## Example

```
RFController(config-captive-portal-test)#webpage external fail
www.brocade.com
RFController(config-captive-portal-test)#
```

## NOTE

The commands `clrscr`, `commit`, `do`, `exit`, `help`, `no`, `revert`, `service`, `show`, and `write` are common commands. For more information, see [Chapter 6, Common Commands](#).

## clear

### *Global Configuration Commands*

Clears parameters, cache entries, table entries, and other similar entries. The clear command is only available for specific commands. The information cleared using this command varies depending on the mode where the clear command is executed.

In this mode, the clear command is used to clear the event history

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
clear event-history
```

### Parameters

---

|               |                          |
|---------------|--------------------------|
| event-history | Clears the event history |
|---------------|--------------------------|

---

### Example

```
RFController(config)#clear event-history  
RFController(config)#
```

## critical-resource-policy

### [Global Configuration Commands](#)

Creates a critical resource monitoring policy. A critical resource is a device (controller, router, gateway, etc.) that is considered critical to the health of the controller managed network. This is a list of IP addresses that are pinged regularly by the wireless controller. If there is a connectivity issue with a device on the critical resource list, an event is generated stating a critical resource is unavailable. The controller does not attempt to restore connection to a critical resource. All critical devices are listed in a critical resource policy.

| Command                                  | Description                                   | Reference                |
|------------------------------------------|-----------------------------------------------|--------------------------|
| <a href="#">critical-resource-policy</a> | Configures captive portal Web page parameters | <a href="#">page 164</a> |

## critical-resource-policy

### Global Configuration Commands

Creates or enters a critical-resource policy. If the defined policy is not present, it is created.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
critical-resource-policy <CRM-Policy>
```

### Parameters

---

|                                 |                                                          |
|---------------------------------|----------------------------------------------------------|
| <code>&lt;CRM-Policy&gt;</code> | Enter a name for the critical resource monitoring policy |
|---------------------------------|----------------------------------------------------------|

---

### Example

```
RFController(config)#critical-resource-policy test
RFController(config-critical-resource-policy-test)#?
commands:
  monitor  Critical resource monitoring
  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
```

## critical-resource-policy-mode

Table 7 Summarizes critical resource monitoring policy commands

**TABLE 7** critical-resource-policy-mode

| Command        | Description                                  | Reference                |
|----------------|----------------------------------------------|--------------------------|
| <i>monitor</i> | Performs critical resource monitoring        | <a href="#">page 166</a> |
| <i>no</i>      | Negates a command or sets its default values | <a href="#">page 167</a> |

**monitor**

*critical-resource-policy-mode*

Performs critical resource monitoring

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
monitor [<IP>|ping-interval <5-86400>]
monitor <IP> ping-mode [arp-icmp|arp-only vlan <1-4094>]
```

**Parameters**

|                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>&lt;IP&gt; ping-mode<br/>[arp-icmp arp-only vlan<br/>&lt;1-4094&gt;]</p> | <p>Enter the IP address of the critical resource to be monitored</p> <ul style="list-style-type: none"> <li>• ping-mode – Enter the protocol used for pinging a critical resource             <ul style="list-style-type: none"> <li>• arp-icmp – Uses either ARP requests or ICMP echo request to monitor a critical resource (requires the AP/Controller to have an IP address)</li> <li>• arp-only – Uses only probing arp requests to monitor a critical resource (suitable for AP/controller without IP address)                 <ul style="list-style-type: none"> <li>• vlan &lt;1-4094&gt; – Enter the VLAN on which the probing ARP request has to be sent</li> </ul> </li> </ul> </li> </ul> |
| <p>ping-interval &lt;5-86400&gt;</p>                                        | <p>Enter the ping interval from 5-86400 seconds</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Example**

```
RFController(config-critical-resource-policy-test)#monitor ping-interval 10
RFController(config-critical-resource-policy-test)#

RFController(config-critical-resource-policy-test)#monitor 172.16.10.2
ping-mode arp-only vlan 1
RFController(config-critical-resource-policy-test)#
```



***no******critical-resource-policy-mode***

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no monitor
```

**Parameters**

---

|         |                                                  |
|---------|--------------------------------------------------|
| monitor | Does not monitor the specified critical resource |
|---------|--------------------------------------------------|

---

**Example**

```
RFController(config-critical-resource-policy-test)#no monitor 172.16.10.2  
RFController(config-critical-resource-policy-test)#
```

## customize

### *Global Configuration Commands*

Customizes the output of summary commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
customize [show-wireless-client|show-wireless-client-stats|
show-wireless-client-stats-rf|show-wireless-radio|
show-wireless-radio-stats|show-wireless-radio-stats-rf]
```

```
customize show-wireless-client
[ap-name|auth|bss|enc|hostname|ip|last-active|location|
mac|radio-alias|radio-id|radio-type|role|role-policy|state|
username|vendor|vlan|wlan]
```

```
customize show-wireless-client-stats [hostname|mac|rx-bytes|
rx-errors|
rx-packets|rx-throughput|tx-bytes|tx-dropped|tx-packets|tx-throughput]
```

```
customize show-wireless-client-stats-rf [average-retry-number|
error-rate|hostname|mac|noise|q-index|rx-rate|signal|snr|t-index|tx-rate]
```

```
customize show-wireless-radio [adopt-to|ap-name|channel|location|
num-clients|power|radio-alias|radio-id|radio-mac|rf-mode|state]
```

```
customize show-wireless-radio-stats [radio-alias|radio-id|radio-mac|
rx-bytes|rx-errors|rx-packets|rx-throughput|tx-bytes|tx-dropped|
tx-packets|tx-throughput]
```

```
customize show-wireless-radio-stats-rf
[average-retry-number|error-rate|noise|q-index|radio-alias|radio-id|radio-mac|
rx-rate|signal|snr|t-index|tx-rate]
```

## Parameters

|                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>show-wireless-client [ap-name   auth   bss   enc   hostn ame   ip   last-active   location   mac     radio-alias   radio-id   radio-type   r ole   role-policy   state   username   vendor   vlan   wlan</pre> | <p>Customizes the output of (show wireless client) commands</p> <ul style="list-style-type: none"> <li>• ap-name – Hostname of the AP to which this client associates</li> <li>• auth – The authentication protocol used by the client</li> <li>• bss – The BSSID to which the client's radio is associated</li> <li>• enc – The encryption suite of the client</li> <li>• hostname – Hostname of the client – Configured by packet sniffing or manually</li> <li>• ip – The IP address of the client</li> <li>• last-active – Displays the last activity seen on the client</li> <li>• location – Location of the AP to which this client is associated</li> <li>• mac – The MAC address of client</li> <li>• radio-alias – Consists of an AP's hostname and the radio interface number in the form of hostname:RX</li> <li>• radio-id – Consists of AP MAC address and the client interface number in the form of AA-BB-CC-DD-EE-FF:RX</li> <li>• radio-type – Radio type of the client</li> <li>• role – The current role of the client</li> <li>• role-policy – The role policy used by the client</li> <li>• state – The current state of the client</li> <li>• username – The username of the client</li> <li>• vendor – The vendor ID of the client</li> <li>• vlan – The VLAN ID assigned to the client</li> <li>• wlan – WLAN name</li> </ul> |
| <pre>show-wirless-client-stats [hostname   mac   rx-bytes   rx-errors   rx-packets   rx-throughput   tx-bytes   tx-dropped   tx-packets   tx-throughput ]</pre>                                                     | <p>Customizes the output of (show wireless client stats) commands</p> <ul style="list-style-type: none"> <li>• hostname – The hstname of the client – Configured by sniffing packets or manually</li> <li>• mac – The MAC address of the client</li> <li>• rx-bytes – Displays the number of bytes received</li> <li>• rx-errors – Displays the number of errors received</li> <li>• rx-packets – Displays the number of packets received</li> <li>• rx-throughput – Displays the number of packets received per port and the percentage of port utilization</li> <li>• tx-bytes – Displays the number of bytes transmitted</li> <li>• tx-dropped – Displays the number of packets dropped during transmission</li> <li>• tx-packets – Displays the total number of packets transmitted</li> <li>• tx-throughput – Displays the number of packets transmitted per port and the percentage of port utilization</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <pre>show-wireless-client-stats-rf [average-retry-number   error-rate   hostname   mac   noise   q-index   rx-rate   signal   snr   t-index   tx-rate]</pre>                                                        | <p>Customizes the output of (show wireless client stats rf) commands</p> <ul style="list-style-type: none"> <li>• average-retry-number – Displays the average retry number per packet</li> <li>• error-rate – Displays the error rate</li> <li>• hostname – Displays the hostname of the client – Configured by sniffing packets or manually</li> <li>• mac – The MAC address of client</li> <li>• noise – Displays the noise level measured in dBm</li> <li>• q-index – Q-Index</li> <li>• rx-rate – Displays the rate of radio packets received</li> <li>• signal – Displays the signal strength in dBm</li> <li>• snr – Displays the Signal to Noise Ratio (SNR) in db</li> <li>• t-index – T-index</li> <li>• tx-rate – Displays the rate at which radio packets are transmitted</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>show-wireless-radio [adopt-to  ap-name channel location  num-clients power  radio-alias radio-id  radio-mac rf-mode state]</pre>                              | <p>Customizes the output of (show wireless radio) commands</p> <ul style="list-style-type: none"> <li>• adopt-to – Displays the name of the Controller to which the client radio is adopted</li> <li>• ap-name – Hostname of the AP to which this radio belongs</li> <li>• channel – The configured and current channel of the radio</li> <li>• location – Location of the AP to which this radio belongs</li> <li>• num-clients – Number of clients associated with this radio</li> <li>• power – The configured and current transmit power of the radio</li> <li>• radio-alias – Consists of the AP's hostname and the radio interface number in the form of hostname:RX</li> <li>• radio-id – Consists of the AP MAC address and the radio interface number in the form of AA-BB-CC-DD-EE-FF:RX</li> <li>• radio-mac – The base MAC address of the radio</li> <li>• rf-mode – The RF mode of the radio (2.4GHz-Wlan/5GHz-wlan/sensor)</li> <li>• state – The current operational state of the radio</li> </ul>                                                             |
| <pre>show-wireless-radio-stats [radio-alias radio-id  radio-mac rx-bytes rx-errors  rx-packets rx-throughput  tx-bytes tx-dropped  tx-packets tx-throughput]</pre> | <p>Customizes the output of (show wireless radio stats) commands</p> <ul style="list-style-type: none"> <li>• radio-alias – Radio alias with AP's hostname and the radio interface number in the form of hostname:RX</li> <li>• radio-id – Consists of the AP MAC address and the radio interface number in the form of AA-BB-CC-DD-EE-FF:RX</li> <li>• radio-mac – The base MAC address of the radio</li> <li>• rx-bytes – Displays the number of bytes received</li> <li>• rx-errors – Displays the number of errors receive</li> <li>• rx-packets – Displays the number of packets received</li> <li>• rx-throughput – Displays the number of packets received per port and the percentage of port utilization</li> <li>• tx-bytes – Displays the number of bytes transmitted</li> <li>• tx-dropped – Displays the number of packets dropped during transmission</li> <li>• tx-packets – Displays the total number of packets transmitted</li> <li>• tx-throughput – Displays the number of packets transmitted per port and the percentage of port utilization</li> </ul> |
| <pre>show-wireless-radio-stats-rf [average-retry-number error-rat e noise q-index radio-alias ra dio-id radio-mac rx-rate signal  snr t-index tx-rate]</pre>       | <p>Customizes the output of (show wireless radio stats rf) commands</p> <ul style="list-style-type: none"> <li>• average-retry-number – Displays the average retry number per packet</li> <li>• error-rate – Displays the error rate</li> <li>• noise – Displays the noise level in dBm</li> <li>• q-index – Q-Index</li> <li>• radio-alias – Consists of the AP's hostname and the radio interface number in the form of hostname:RX</li> <li>• radio-id – Radio ID with the AP MAC address and the radio interface number in the form of AA-BB-CC-DD-EE-FF:RX</li> <li>• radio-mac – The base MAC address of the radio</li> <li>• rx-rate – Displays the rate of radio packets received</li> <li>• signal – Displays the signal strength in dBm</li> <li>• snr – Displays the Signal to Noise Ratio in db</li> <li>• t-index – T-Index</li> <li>• tx-rate – Displays the rate at which radio packets are transmitted</li> </ul>                                                                                                                                             |

**Example**

```
RFController(config)#customize show-wireless-client ap-name auth
RFController(config)#
```

```
RFController(config)#customize show-wireless-client-stats mac
RFController(config)#
```

```
RFController(config)#customize show-wireless-client-stats-rf
average-retry-number
RFController(config)#
```

```
RFController(config)#customize show-wireless-radio adopt-to
RFController(config)#
```

```
RFController(config)#customize show-wireless-radio-stats radio-mac
RFController(config)#
```

## device

### Global Configuration Commands

Specifies configuration on multiple devices

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
device {containing/filter}
device containing <HOSTNAME> {filter type [br650|br6511|br6532|
br71xx|rfs4000|rfs6000|rfs7000]}
device filter type [br650|br6511|br6532|br71xx1|rfs4000|
rfs6000|rfs7000]
```

### Parameters

---

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {containing filter} | <ul style="list-style-type: none"> <li>• containing &lt;HOSTNAME&gt; filter type [br650 br6511 br6532 br71xx rfs4000 rfs6000 rfs7000] - Optional. Specifies the devices that contain a sub-string in the host-name</li> <li>• filter type - Specify the additional selection filter by device type from the list of devices <ul style="list-style-type: none"> <li>• br650 - Mobility 650 Access Point profile</li> <li>• br6511 - Mobility 6511 Access Point profile</li> <li>• br6532 - Mobility 6532 Access Point profile</li> <li>• br7131 - Mobility 7131 Series Access Point profile</li> <li>• rfs4000 - Mobility RFS4000 wireless controller profile</li> <li>• rfs6000 - Mobility RFS6000 wireless controller profile</li> <li>• rfs7000 - Mobility RFS7000 wireless controller profile</li> </ul> </li> </ul> |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#device containing ap filter type br7131
% Error: Parsing cmd line (1)
RFController(config)#
```

## device-categorization

### [Global Configuration Commands](#)

Categorizes devices based on different parameters.

| Command                               | Description                                 | Reference                |
|---------------------------------------|---------------------------------------------|--------------------------|
| <a href="#">device-categorization</a> | Configures the device categorization lists. | <a href="#">page 174</a> |

## device-categorization

### *Global Configuration Commands*

Configures a device categorization object

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
device-categorization <device-categorization-name>
```

### Parameters

---

|                                                 |                                                |
|-------------------------------------------------|------------------------------------------------|
| <code>&lt;device-categorization-name&gt;</code> | Defines the name of device categorization list |
|-------------------------------------------------|------------------------------------------------|

---

### Example

```
RFController(config)#device-categorization rfs7000
RFController(config)#

RFController(config-device-categorization-rfs7000)#?
Device Category Mode commands:
 mark-device  Add a device
 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
```



## device-categorization-mode commands

Table 8 Summarizes device-categorization mode commands

**TABLE 8** device-categorization-mode commands

| Command            | Description                                     | Reference                |
|--------------------|-------------------------------------------------|--------------------------|
| <i>mark-device</i> | Adds a device to the device categorization list | <a href="#">page 176</a> |
| <i>no</i>          | Negates a command or sets its default values    | <a href="#">page 177</a> |

***mark-device****device-categorization-mode commands*

Adds a device to the device categorization list

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
mark-device [sanctioned|neighboring]
mark-device [sanctioned|neighboring] [ap|client]
mark-device [sanctioned|neighboring] ap [<MAC>|any] ssid [<WORD>|any]
mark-device [sanctioned|neighboring] client [<MAC>|any]
```

**Parameters**

[sanctioned|  
neighboring] [ap [<MAC>  
|any]|station  
[<MAC> |any]

- sanctioned – Marks an authorized device
- neighboring – Marks a neighboring device

The following parameters are common for the above:

- ap [<MAC> |any] – Enter the MAC address of an AP
  - <MAC> ssid [<WORD>|any] – Enter an AP MAC address
  - any ssid [<WORD>|any] – Enter any AP MAC address
    - ssid [<WORD>|any] – Enter a particular SSID value or any SSID
- client [<MAC> |any] – Enter a client MAC address
  - <MAC> – Enter a particular client MAC address
  - any – Any station (client) MAC address

**Example**

```
RFController(config-device-categorization-rfs7000)#mark-device sanctioned ap
any ssid any
RFController(config-device-categorization-rfs7000)#

RFController(config-device-categorization-rfs7000)#mark-device neighboring
client 11-22-33-44-55-66
RFController(config-device-categorization-rfs7000)#
```

**no***device-categorization-mode commands*

Removes a device from the network

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no mark-device
```

**Parameters**

---

|             |                  |
|-------------|------------------|
| mark-device | Removes a device |
|-------------|------------------|

---

**Example**

```
RFController(config-device-categorization-rfs7000)#no mark-device authorized
ap any ssid 1
%% Error: Parsing cmd line
RFController(config-device-categorization-rfs7000)#
```

**NOTE**

The commands `clear`, `commit`, `do`, `exit`, `help`, `write`, `revert`, `service` and `show` are common commands. For more information, see [Chapter 6, Common Commands](#).

---

## dhcp-server-policy

### *Global Configuration Commands*

Configures a DHCP Server policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dhcp-server-policy <dhcp-policy -name>
```

### **Parameters**

---

|                    |                                              |
|--------------------|----------------------------------------------|
| <dhcp-policy-name> | Enter a DHCP server policy name to configure |
|--------------------|----------------------------------------------|

---

### **Example**

```
RFController(config)#dhcp-server-policy test
RFController(config)#?
```

---

### **NOTE**

For more information, see [Chapter 14, dhcp-server-policy](#).

---

## dns-whitelist

### [Global Configuration Commands](#)

Configures a whitelist of devices permitted to access the controller managed network or a hotspot configured for the controller managed network.

| Command                       | Description                   | Reference                |
|-------------------------------|-------------------------------|--------------------------|
| <a href="#">dns-whitelist</a> | Configures the DNS whitelist. | <a href="#">page 180</a> |

## dns-whitelist

### Global Configuration Commands

Configures a DNS whitelist

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
dns-whitelist <DNS-WHITELIST>
```

### Parameters

---

|                 |                                                                            |
|-----------------|----------------------------------------------------------------------------|
| <DNS-WHITELIST> | Enter the name of whitelist (will be created if it does not already exist) |
|-----------------|----------------------------------------------------------------------------|

---

### Example

```
RFController(config-dns-whitelist-test)#?  
DNS Whitelist Mode commands:  
no          Negate a command or set its defaults  
permit     Match a host  
  
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  
  
RFController(config-dns-whitelist-test)#
```

## dns-whitelist mode commands

Table 9 Summarizes dns-whitelist mode commands

**TABLE 9** dns-whitelist mode commands

| Command       | Description                                  | Reference                |
|---------------|----------------------------------------------|--------------------------|
| <i>permit</i> | Matches a host                               | <a href="#">page 182</a> |
| <i>no</i>     | Negates a command or sets its default values | <a href="#">page 183</a> |

## *permit*

### *dns-whitelist mode commands*

A whitelist is a list of host names and IP addresses permitted access to the controller managed network or captive portal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
permit <WORD> {suffix}
```

### **Parameters**

---

|                 |                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WORD> {suffix} | Permits a list of hostnames or IP addresses access to the controller managed network or hotspot <ul style="list-style-type: none"><li>• &lt;WORD&gt; - the host name or IP address of the device being permitted access.</li><li>• suffix - Matches any hostname including the specified na</li></ul> |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-dns-whitelist-test)#permit brocade.com suffix
RFController(config-dns-whitelist-test)#show context
dns-whitelist test
  permit brocade.com suffix
RFController(config-dns-whitelist-test)#
```



***no******dns-whitelist mode commands***

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no permit <WORD>
```

**Parameters**

---

|                  |                                                                                   |
|------------------|-----------------------------------------------------------------------------------|
| no permit <WORD> | Does not match the hostname or IP address in the list and is not permitted access |
|------------------|-----------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-dns-whitelist-test)#no permit brocade.com  
RFController(config-dns-whitelist-test)#
```

## do

### *Global Configuration Commands*

Runs commands from the EXEC mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
do <parameter>
```

### Parameters

---

|   |                                                                                  |
|---|----------------------------------------------------------------------------------|
| ? | Displays the parameters for which information can be viewed using the do command |
|---|----------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#do ?
  ap-upgrade      AP firmware upgrade
  archive         Manage archive files
  boot            Boot commands
  cd              Change current directory
  change-passwd   Change password
  clear           Clear
  clock           Configure software system clock
  cluster         Cluster commands
  commit         Commit all changes made in this session
  configure       Enter configuration mode
  connect         Open a console connection to a remote device
  copy            Copy from one file to another
  crypto          Encryption related commands
  debug          Debugging functions
  delete          Deletes specified file from the system.
  diff            Display differences between two files
  dir             List files on a filesystem
  disable         Turn off privileged mode command
  edit            Edit a text file
  enable         Turn on privileged mode command
  erase           Erase a filesystem
  format          Format file system
  halt           Halt the system
  help           Description of the interactive help system
  logging         Modify message logging facilities
  mint           MiNT protocol
  mkdir           Create a directory
  more           Display the contents of a file
  no             Negate a command or set its defaults
```

|               |                                                                                     |
|---------------|-------------------------------------------------------------------------------------|
| page          | Toggle paging                                                                       |
| ping          | Send ICMP echo messages                                                             |
| pwd           | Display current directory                                                           |
| reload        | Halt and perform a warm reboot                                                      |
| remote-debug  | Troubleshoot remote system(s)                                                       |
| rename        | Rename a file                                                                       |
| revert        | Revert changes                                                                      |
| rmdir         | Delete a directory                                                                  |
| self          | Config context of the device currently logged into                                  |
| telnet        | Open a telnet connection                                                            |
| terminal      | Set terminal line parameters                                                        |
| time-it       | Check how long a particular command took between request and completion of response |
| tracert       | Trace route to destination                                                          |
| upgrade       | Upgrade software image                                                              |
| upgrade-abort | Abort an ongoing upgrade                                                            |
| watch         | Repeat the specific CLI command at a periodic interval                              |
| write         | Write running configuration to memory or terminal                                   |
| clrscr        | Clears the display screen                                                           |
| exit          | Exit from the CLI                                                                   |
| service       | Service Commands                                                                    |
| show          | Show running system information                                                     |

### end

#### *Global Configuration Commands*

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to the previous mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
end
```

#### **Parameters**

None

#### **Example**

```
RFController(config)#end  
RFController#
```

## event-system-policy

### [Global Configuration Commands](#)

Configures a policy which configures how events are handled by the wireless controller. Each event can be configured individually to perform an action such as sending an email or forwarding a notification to its parent controller.

| Command                             | Description                         | Reference                |
|-------------------------------------|-------------------------------------|--------------------------|
| <a href="#">event-system-policy</a> | Configures the event-system-policy. | <a href="#">page 188</a> |

## event-system-policy

### Global Configuration Commands

Configures an event system policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
event-system-policy <EVENT-SYSTEM-POLICY>
```

### Parameters

---

|                                          |                                                                                      |
|------------------------------------------|--------------------------------------------------------------------------------------|
| <code>&lt;EVENT-SYSTEM-POLICY&gt;</code> | Enter the name of event system policy (will be created if it does not already exist) |
|------------------------------------------|--------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#event-system-policy event-testpolicy
RFController(config-event-system-policy-event-testpolicy)#?
Event System Policy Mode commands:
  event      Configure an event
  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

RFController(config-event-system-policy-event-testpolicy)#
```

## event-system-policy mode commands

[Table 10](#) Summarizes event system policy mode commands

**TABLE 10** event-system-policy mode commands

| Command               | Description                                  | Reference                |
|-----------------------|----------------------------------------------|--------------------------|
| <a href="#">event</a> | Configures an event                          | <a href="#">page 190</a> |
| <a href="#">no</a>    | Negates a command or sets its default values | <a href="#">page 198</a> |

### *event*

#### *event-system-policy mode commands*

Configures an event

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
event [<event type>] [<event name>] [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

---

#### **NOTE**

The parameter values for the <event type> and <event name> are summarized in the table under the Parameters section.

---



**Parameters**

| <event type> | <event name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aaa          | <ul style="list-style-type: none"> <li>• radius-discon-msg – RADIUS disconnection message</li> <li>• radius-session-expired – RADIUS session expired message</li> <li>• radius-session-not-started – RADIUS session not started message</li> <li>• radius-vlan-update – RADIUS VLAN update message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| adv-wips     | <ul style="list-style-type: none"> <li>• adv-wips-event-1 – Event adv-wips-event-1 message</li> <li>• adv-wips-event-10 – Event adv-wips-event-10 message</li> <li>• adv-wips-event-105 – Event adv-wips-event-105 message</li> <li>• adv-wips-event-109 – Event adv-wips-event-109 message</li> <li>• adv-wips-event-11 – Event adv-wips-event-11 message</li> <li>• adv-wips-event-110 – Event adv-wips-event-110 message</li> <li>• adv-wips-event-111 – Event adv-wips-event-111 message</li> <li>• adv-wips-event-112 – Event adv-wips-event-112 message</li> <li>• adv-wips-event-113 – Event adv-wips-event-113 message</li> <li>• adv-wips-event-114 – Event adv-wips-event-114 message</li> <li>• adv-wips-event-115 – Event adv-wips-event-115 message</li> <li>• adv-wips-event-116 – Event adv-wips-event-116 message</li> <li>• adv-wips-event-117 – Event adv-wips-event-117 message</li> <li>• adv-wips-event-118 – Event adv-wips-event-118 message</li> <li>• adv-wips-event-119 – Event adv-wips-event-119 message</li> <li>• adv-wips-event-12 – Event adv-wips-event-12 message</li> <li>• adv-wips-event-120 – Event adv-wips-event-120 message</li> <li>• adv-wips-event-121 – Event adv-wips-event-121 message</li> <li>• adv-wips-event-13 – Event adv-wips-event-13 message</li> <li>• adv-wips-event-14 – Event adv-wips-event-14 message</li> <li>• adv-wips-event-142 – Event adv-wips-event-142 message</li> <li>• adv-wips-event-16 – Event adv-wips-event-16 message</li> <li>• adv-wips-event-19 – Event adv-wips-event-19 message</li> <li>• adv-wips-event-2 – Event adv-wips-event-2 message</li> <li>• adv-wips-event-21 – Event adv-wips-event-21message</li> <li>• adv-wips-event-220 – Event adv-wips-event-220 message</li> <li>• adv-wips-event-221 – Event adv-wips-event-221 message</li> <li>• adv-wips-event-222 – Event adv-wips-event-222 message</li> <li>• adv-wips-event-25 – Event adv-wips-event-25 message</li> <li>• adv-wips-event-26 – Event adv-wips-event-26 message</li> <li>• adv-wips-event-29 – Event adv-wips-event-29 message</li> <li>• adv-wips-event-3 – Event adv-wips-event-3 message</li> <li>• adv-wips-event-47 – Event adv-wips-event-47 message</li> <li>• adv-wips-event-63 – Event adv-wips-event-63 message</li> <li>• adv-wips-event-87 – Event adv-wips-event-87 message</li> </ul> |

| <event type>   | <event name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap             | <ul style="list-style-type: none"> <li>• adopted – Event adopted message</li> <li>• adopted-to-switch – Event adopted to controller message</li> <li>• ap-autoup-done –Event ap autoup done message</li> <li>• ap-autoup-fail – Event ap autoup fail message</li> <li>• ap-autoup-needed – Event ap autoup needed message</li> <li>• ap-autoup-no-need – Event ap autoup not needed message</li> <li>• ap-autoup-reboot – Event ap autoup reboot message</li> <li>• ap-autoup-timeout – Event ap autoup timeout message</li> <li>• ap-autoup-ver – Event ap autoup version message</li> <li>• image-parse-failure – Event image parse failure message</li> <li>• legacy-auto-update – Event legacy auto update message</li> <li>• no-image-file – Event no image file message</li> <li>• reset – Event reset message</li> <li>• sw-conn-lost – Event software connection lost message</li> <li>• unadopted – Event unadopted message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| captive-portal | <ul style="list-style-type: none"> <li>• allow-access – Event allow access message</li> <li>• auth-failed – Event authentication failed message</li> <li>• auth-success – Event authentication success message</li> <li>• client-disconnect – Event client disconnected message</li> <li>• client-removed – Event client removed message</li> <li>• flex-log-access – Event flexible log access message</li> <li>• inactivity-timeout – Event inactivity timeout message</li> <li>• purge-client – Event purge client message</li> <li>• session-timeout – Event session timeout message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| certmgr        | <ul style="list-style-type: none"> <li>• ca-cert-actions-failure – Event ca certificate actions failure message</li> <li>• ca-cert-actions-success – Event ca certificate actions success message</li> <li>• ca-key-actions-failure – Event ca key actions failure message</li> <li>• ca-key-actions-success – Event ca key actions success message</li> <li>• cert-expiry – Event certificate expiry message</li> <li>• crl-actions-failure – Event crl (<i>Certificate Revocation List</i>) actions failure message</li> <li>• crl-actions-success – Event crl (<i>Certificate Revocation List</i>) actions success message</li> <li>• csr-export-failure – Event csr (<i>Certificate Server Request</i>) export failure message</li> <li>• csr-export-success – Event csr (<i>Certificate Server Request</i>) export success message</li> <li>• delete-trustpoint-action – Event delete trustpoint action message</li> <li>• export-trustpoint – Event export trustpoint message</li> <li>• import-trustpoint – Event import trustpoint message</li> <li>• rsa-key-actions-failure – Event RSA key actions failure message</li> <li>• rsa-key-actions-success – Event RSAkey actions success message</li> <li>• srv-cert-actions-success – Event server certificate actions success message</li> <li>• svr-cert-actions-failure – Event server certificate actions failure message</li> </ul> |
| cfgd           | <ul style="list-style-type: none"> <li>• acl-attached-altered – Event acl attached altered message</li> <li>• acl-rule-altered – Event acl rule altered message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| cluster        | <ul style="list-style-type: none"> <li>• max-exceeded – Event maximum exceeded message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| crm            | <p data-bbox="631 1705 959 1726">Event Critical Resource Monitoring</p> <ul style="list-style-type: none"> <li>• critical-resource-down – Event Critical Resource Down</li> <li>• critical-resource-up – Event Critical Resource Up</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| <event type> | <event name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dhcpcsvr     | <ul style="list-style-type: none"> <li>• dhcp-start</li> <li>• dhcpcsvr-stop – Event DHCP sever stopped</li> <li>• relayifacenoip – Event relay interface no IP message</li> <li>• relaynoiface – Event relay no interface message</li> <li>• relay-start – Event relay agent started</li> <li>• relay-stop – Event DHCP relay agent stopped</li> <li>•</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| diag         | <ul style="list-style-type: none"> <li>• autogen-tech-sprt – Event autogen technical support message</li> <li>• buf-usage – Event buffer usage message</li> <li>• cpu-load – Event CPU load message</li> <li>• disk-usage – Event disk usage message</li> <li>• elapsed-time – Event elapsed time message</li> <li>• fan-underspeed – Event fan underspeed message</li> <li>• fd-count – Event forward count message</li> <li>• free-flash-disk – Event free flash disk message</li> <li>• free-flash-inodes – Event free flash inodes message</li> <li>• free-nvram-disk – Event free nvram disk message</li> <li>• free-nvram-inodes – Event free nvram inodes message</li> <li>• free-ram – Event free ram message</li> <li>• free-ram-disk – Event free ram disk message</li> <li>• free-ram-inodes – Event free ram inodes message</li> <li>• head-cache-usage – Event head cache usage message</li> <li>• high-temp – Event high temp message</li> <li>• ip-dest-usage – Event ip destination usage message</li> <li>• led-identify – Event led identify message</li> <li>• low-temp – Event low temp message</li> <li>• new-led-state – Event new led state message</li> <li>• over-temp – Event over temp message</li> <li>• over-voltage – Event over voltage message</li> <li>• poe-init-fail – Event PoE init fail message</li> <li>• poe-power-level – Event PoE power level message</li> <li>• poe-read-fail – Event PoE read fail message</li> <li>• poe-state-change – Event PoE state change message</li> <li>• ram-usage – Event ram usage message</li> <li>• under-voltage – Event under voltage message</li> <li>• wd-reset-sys – Event wd reset system message</li> <li>• wd-state-change – Event wd state change message</li> </ul> |

| <event type> | <event name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot11        | <ul style="list-style-type: none"> <li>• client-associated – Wireless client associated event message</li> <li>• client-denied-assoc – Event client denied association message</li> <li>• client-disassociated – Wireless client disassociated message</li> <li>• country-code – Event country code message</li> <li>• country-code-error – Event country code error message</li> <li>• eap-cached-keys – Event EAP cached keys message</li> <li>• eap-client-timeout – Event EAP client timeout message</li> <li>• eap-failed – Event EAP failed message</li> <li>• eap-opp-cached-keys – Event EAP opp cached keys message</li> <li>• eap-preauth-client-timeout – Event eap preauthentication client timeout message</li> <li>• eap-preauth-failed – Event EAP preauthentication failed message</li> <li>• eap-preauth-server-timeout – Event EAP preauthentication server timeout message</li> <li>• eap-preauth-success – Event EAP preauthentication success message</li> <li>• eap-server-timeout – Event EAP server timeout message</li> <li>• eap-success – Event EAP success message</li> <li>• kerberos-client-failed – Event kerberos client failed message</li> <li>• kerberos-client-success – Event kerberos client success message</li> <li>• kerberos-wlan-failed – Event kerberos WLAN failed message</li> <li>• kerberos-wlan-success – Event kerberos WLAN success message</li> <li>• kerberos-wlan-timeout – Event kerberos WLAN timeout message</li> <li>• tkip-cntrmeas-end – Event TKIP cntrmeas end message</li> <li>• tkip-cntrmeas-start – Event TKIP cntrmeas start message</li> <li>• tkip-mic-fail-report – Event TKIP mic fail report message</li> <li>• tkip-mic-failure – Event TKIP mic failure message</li> <li>• unsanctioned-ap-active – Event unsanctioned AP active message</li> <li>• unsanctioned-ap-inactive – Event unsanctioned AP inactive message</li> <li>• unsanctioned-ap-status-change – Event unsanctioned AP status change</li> <li>• voice-call-completed – Event voice call completed message</li> <li>• voice-call-failed – Event voice call failed message</li> <li>• wpa-wpa2-failed – Event WPA-WPA2 failed message</li> <li>• wpa-wpa2-key-rotn – Event WPA-WPA2 key rotn message</li> <li>• wpa-wpa2-success – Event WPA-WPA2 success message</li> </ul> |
| dpd2         | <ul style="list-style-type: none"> <li>• crm-critical-resource-down – Event CRM critical resource down message</li> <li>• crm-critical-resource-up – Event CRM critical resource up message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| filegmt      | <ul style="list-style-type: none"> <li>• http – Event HTTP message</li> <li>• httplocal – Event HTTP local message</li> <li>• https-start – Event HTTPS start message</li> <li>• https-wait – Event HTTPS wait message</li> <li>• httpstart – Event HTTP start message</li> <li>• keyadded – Event key added message</li> <li>• keydeleted – Event key deleted message</li> <li>• trustpointdeleted – Event trust point deleted message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| <event type> | <event name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fwu          | <ul style="list-style-type: none"> <li>• fwuaborted – Event fwu aborted message</li> <li>• fwubadconfig – Event fwu bad config message</li> <li>• fwucorruptedfile – Event fwu corrupted file message</li> <li>• fwucouldntgetfile – Event fwu could not get file message</li> <li>• fwudone – Event fwu done message</li> <li>• fwufileundef – Event fwu file undefined message</li> <li>• fwunoneed – Event fwu no need message</li> <li>• fwuprodmismatch – Event fwu prod mismatch message</li> <li>• fwuserverundef – Event fwu server undefined message</li> <li>• fwuserverunreachable – Event fwu server unreachable message</li> <li>• fwusignmismatch – Event fwu signature mismatch message</li> <li>• fwusyserr – Event fwu system error message</li> <li>• fwuunsupportedhw – Event fwu unsupported hardware message</li> <li>• fwuvermismatch – Event fwu version mismatch message</li> </ul> |
| licmgr       | <ul style="list-style-type: none"> <li>• licbaddata – Event license bad data message</li> <li>• licbadfeature – Event license bad feature message</li> <li>• licbadproduct – Event license bad product message</li> <li>• licexpired – Event license expired message</li> <li>• licincompdata – Event license incomplete data message</li> <li>• licmodified – Event license modified message</li> <li>• newlicense – Event new license message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| mesh         | <ul style="list-style-type: none"> <li>• mesh-link-down – Event mesh link down message</li> <li>• mesh-link-up – Event mesh link up message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| nsm          | <ul style="list-style-type: none"> <li>• dhcperr – Event DHCP certification error message</li> <li>• dhcpdefrt – Event DHCP defrt message</li> <li>• dhcpip – Event DHCP IP message</li> <li>• dhcpipchg – Event DHCP IP change message</li> <li>• dhcpipnoadd – Event DHCP IP no add message</li> <li>• dhcpnodefrt – Event DHCP no defrt message</li> <li>• ifdown – Event if down message</li> <li>• ifipcfg – Event if IP config message</li> <li>• ifup – Event If up message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                               |
| pm           | <ul style="list-style-type: none"> <li>• procid – Event procid message</li> <li>• procmaxstrtr – Event proc max restart message</li> <li>• procnorep – Event proc no response message</li> <li>• procrstrtr – Event proc restart message</li> <li>• procstart – Event proc start message</li> <li>• procstop – Event proc stop message</li> <li>• procsysrstrtr – Event proc system restart message</li> <li>• startupcomplete – Event startup complete message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| radconf      | raduserpassstrength – Event RADIUS user pass strength message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| radio        | <ul style="list-style-type: none"> <li>• radar-detected – Event radar detected message</li> <li>• radar-scan-completed – Event radar scan completed message</li> <li>• radar-scan-started – Event radar scan started message</li> <li>• radio-state-change – Event radio state change message</li> <li>• resume-home-channel – Event resume home channel message</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## 5 Global Configuration Commands

| <b>&lt;event type&gt;</b> | <b>&lt;event name&gt;</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rns                       | <ul style="list-style-type: none"> <li>• adaptererr – Event adapter error message</li> <li>• adapterstatechange – Event adapter state change message</li> <li>• adapterstatus – Event adapter status message</li> <li>• adaptertag – Event adapter tag message</li> <li>• alelicensemissing –Event ale license missing message</li> <li>• devicestatechange – Event device state change message</li> <li>• taglocation – Event tag location message</li> </ul>                                                                                                                                                                    |
| securitymgr               | <ul style="list-style-type: none"> <li>• deprecatedcli – Event deprecated cli message</li> <li>• fatal-hit – Event fatal hit message</li> <li>• log-cli-error – Event log cli error message</li> <li>• userpasstrength – Event user pass strength message</li> </ul>                                                                                                                                                                                                                                                                                                                                                              |
| smrt                      | <ul style="list-style-type: none"> <li>• calibration-done – Event calibration done message</li> <li>• calibration-started – Event calibration started message</li> <li>• config-cleared – Configuration cleared event message</li> <li>• cov-hole-recovery – Event coverage hole recovery message</li> <li>• cov-hole-recovery-done – Event coverage hole recovery done message</li> <li>• interference-recovery – Event interference recovery message</li> <li>• neighbor-recovery – Event neighbor recovery message</li> <li>• power-adjustment – Event power adjustment message</li> </ul>                                     |
| smtpnot                   | <ul style="list-style-type: none"> <li>• cfg – Event cfg message</li> <li>• cfginc – Event cfg inc message</li> <li>• net – Event net message</li> <li>• proto – Event proto message</li> <li>• smtpauth – Event SMTP authentication message</li> <li>• smtperr – Event SMTP error message</li> <li>• smtpinfo – Event SMTP information message</li> </ul>                                                                                                                                                                                                                                                                        |
| snmpd                     | <ul style="list-style-type: none"> <li>• opnotreceivemessage – Event op not received message</li> <li>• otherrequed – Event other request qued message</li> <li>• setqued – Event set qued message</li> <li>• snmpsetbindingaudit – Event SNMP set binding audit message</li> <li>• snmpsetfailureaudit – Event SNMP set failure audit message</li> <li>• snmpsetsuccessaudit – Event SNMP set success audit message</li> <li>• v12autherror – Event v12 authentication error message</li> <li>• v3autherror – Event v3 authentication error message</li> <li>• vacmnosuchcontext – Event vacm no such context message</li> </ul> |
| sole                      | <ul style="list-style-type: none"> <li>• adapterdataerr – Event adapter data error message</li> <li>• adaptererr – Event adapter error message</li> <li>• adapterevent – Event adapter event message</li> <li>• adapterstatechange – Event adapter state change message</li> </ul>                                                                                                                                                                                                                                                                                                                                                |
| ssm                       | countrycode – Event country code message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| <event type>      | <event name>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| system            | <ul style="list-style-type: none"> <li>• clock-reset – Event clock reset message</li> <li>• http – Event HTTP message</li> <li>• login – Event login message</li> <li>• login-fail – Event login fail message</li> <li>• login-fail-access – Event login fail access message</li> <li>• login-fail-bad-role – Event login fail bad role message</li> <li>• logout – Event logout message</li> <li>• panic – Event panic message</li> <li>• procstop – Event proc stop message</li> <li>• system-autoup-disable – Event system autoup disable message</li> <li>• system-autoup-enable – Event system autoup enable message</li> <li>• ui-user-auth-fail – Event ui user authentication fail message</li> <li>• ui-user-auth-success – Event ui user authentication success message</li> </ul> |
| test              | <ul style="list-style-type: none"> <li>• testalert – Event test alert message</li> <li>• testargs – Event test arguments message</li> <li>• testcrit – Event test critical message</li> <li>• testdebug – Event test debug message</li> <li>• testemerg – Event test emergency message</li> <li>• testerr – Event test error message</li> <li>• testinfo – Event test information message</li> <li>• testnotice – Event test notice message</li> <li>• testwarn – Event test warning message</li> </ul>                                                                                                                                                                                                                                                                                      |
| wips              | <ul style="list-style-type: none"> <li>• wips-client-blacklisted – Event WIPS client blacklisted message</li> <li>• wips-client-rem-blacklist – Event WIPS client rem blacklist message</li> <li>• wips-event – Event WIPS event</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| email             | Email notifications                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| forward-to-switch | Forward                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| snmp              | SNMP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| syslog            | Syslog                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| default           | Default                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| off               | Off                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| on                | On                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

### Example

```

RFController(config-event-system-policy-event-testpolicy)#event aaa
radius-discon-msg email on forward-to-switch default snmp default syslog
default
RFController(config-event-system-policy-event-testpolicy)#
RFController(config-event-system-policy-adv-wips)#event adv-wips
adv-wips-event-63 forward-to-switch default syslog on snmp on email on
RFController(config-event-system-policy-adv-wips)#

RFController(config-event-system-policy-testpolicy)#show context
event-system-policy testpolicy
  event sole adaptererr syslog off snmp off forward-to-switch off
RFController(config-event-system-policy-testpolicy)#

```

### *no*

#### *event-system-policy mode commands*

Negates an event configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
no [<event type>] [<event name>] [email|forward-to-switch|snmp|syslog]
[default|on|off]
```

#### **Parameters**

None

#### **Example**

```
RFController(config-event-system-policy-testpolicy)#
RFController(config-event-system-policy-testpolicy)#no event aaa
% Error: event_system_policy[aaa] does not exist, unable to delete
RFController(config)#
```



## firewall-policy

### *Global Configuration Commands*

Configures a firewall policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
firewall-policy <firewall-policy-name>
```

### **Parameters**

---

|                        |                                           |
|------------------------|-------------------------------------------|
| <firewall-policy-name> | Enter a firewall policy name to configure |
|------------------------|-------------------------------------------|

---

### **Example**

```
RFController(config)#firewall-policy test
RFController(config-fw-policy-test)#
```

---

### **NOTE**

For more information, see [Chapter 15, firewall-policy](#).

---

## help

### *Global Configuration Commands*

Describes the interactive help system.

Use this command to access the advanced help feature. Use “?” anytime at the command prompt to access a help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
help {search} <WORD> {detailed|only-show|skip-show}
```

### Parameters

---

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {search} <WORD>                | Searches for CLI commands related to a specific term                                                                                                                                                                                                                                                                                                                                                                                              |
| {detailed only-show skip-show} | <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Enter a term to search CLI commands (Eg: a feature or a configuration parameter)<ul style="list-style-type: none"><li>• detailed – Searches and displays help strings in addition to mode and commands</li><li>• only-show – Displays only "show" commands, not configuration commands</li><li>• skip-show – Displays only configuration commands, not "show" commands</li></ul></li></ul> |

---

**Example**

```

Mode      : Priv Exec
Command : show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
          \ Show running system information
          \ Debugging functions
          \ Wireless Module
          \ On AP/Controller or RF-Domain
          \ AP / Controller / RF-Domain name

: show adoption info (|(on DEVICE-NAME))
  \ Show running system information
  \ Display information related to adoption to wireless controller
  \ Display adoption status of this device and its adopted access
point
  \ On AP/Controller
  \ AP / Controller name

: show adoption offline
  \ Show running system information
  \ Display all information related to unadopted to wireless
controller
  \ Display unadopted status of this device and its adopted access
point

: show wireless ap (|(on DEVICE-OR-DOMAIN-NAME))
  \ Show running system information
  \ Wireless commands
  \ Information regarding managed Access Points
  \ On AP/Controller or RF-Domain
  \ AP / Controller / RF-Domain name

: show wireless ap configured
  \ Show running system information
  \ Wireless commands
  \ Information regarding managed Access Points
  \ Information of all Access Points in configuration

: show wireless ap detail (|WORD)
  \ Show running system information
  \ Wireless commands
  \ Information regarding managed Access Points
  \ detailed information for given AP
  \ AP mac address or its hostname

: show wireless unsanctioned aps (|(on DEVICE-OR-DOMAIN-NAME))
  \ Show running system information
--More--
RFController(config)#

```

## host

### *Global Configuration Commands*

Enters the configuration context of a remote device using its hostname.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
host <DEVICE-NAME>
```

### **Parameters**

---

|               |                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------|
| <DEVICE-NAME> | The name of the controller. This name is displayed when the controller is accessed from any network. |
|---------------|------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config)#host  
RFController                               RFDOMAIN_UseCase1/37FAAA  
RFController(config)#host RFDOMAIN_UseCase1/37FAAA  
RFController(config-device-00-15-70-37-FA-AA)#
```

## igmp-snoop-policy

### *Global Configuration Commands*

Configures an igmp-snoop policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
igmp-snoop-policy <igmp-snoop-policy -name>
```

### Parameters

---

|                          |                                             |
|--------------------------|---------------------------------------------|
| <igmp-snoop-policy-name> | Enter a igmp-snoop policy name to configure |
|--------------------------|---------------------------------------------|

---

### Example

```
RFController(config)#igmp-snoop-policy test
RFController(config)#?
```

---

### NOTE

For more information, see [Chapter 16, igmp-snoop-policy](#).

---

## ip

### [Global Configuration Commands](#)

Configures a selected *Internet Protocol* (IP) component

Access-lists define access to the controller managed network using a set of rules. Each rule specifies an action taken when a packet matches a given set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. The controller supports the following ACLs:

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ip access-list <IP-ACCESS-LIST>
```

### Parameters

---

|                              |                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|
| access-list <IP-ACCESS-LIST> | Configures an access-list                                                                                         |
|                              | <ul style="list-style-type: none"><li>• &lt;IP-ACCESS-LIST&gt; - Enter the name of the ACL to configure</li></ul> |

---

### Example

```
RFController(config)#ip access-list test ?
RFController(config)#
```

### NOTE

For more information, see [Chapter 13, access-list](#).

---

## mac

### [Global Configuration Commands](#)

Configures MAC access lists (goes to the MAC ACL mode)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mac access-list <MAC-ACCESS-LIST>
```

### Parameters

---

|                               |                                                   |
|-------------------------------|---------------------------------------------------|
| access-list <MAC-ACCESS-LIST> | Defines the ACL configuration for the MAC address |
| • <MAC-ACCESS-LIST>           | - Defines the name of the ACL                     |

---

### Usage Guidelines

To delete MAC ACL, use *no access-list <access-list name>* under the Global Config mode.

### Example

```
RFController(config)#mac access-list test1
RFController(config)#
```

---

### NOTE

When using the mac access-list parameter, enter the following contexts:

```
RFController(config)#mac access-list <access-list-name>
RFController(config-mac-acl-test1)#
```

For more information, see [Chapter 13, access-list](#).

---

## management-policy

### *Global Configuration Commands*

Configures a management policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
management-policy <management-policy-name>
```

### **Parameters**

---

|                          |                                             |
|--------------------------|---------------------------------------------|
| <management-policy-name> | Enter a management policy name to configure |
|--------------------------|---------------------------------------------|

---

### **Example**

```
RFController(config)#management-policy test
RFController(config-management-policy-test)#
```

---

### **NOTE**

For more information, see [Chapter 18, management-policy](#).

---



## mint-policy

### *Global Configuration Commands*

Configures the global MiNT policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
mint-policy global-default
```

### **Parameters**

---

|                    |                                       |
|--------------------|---------------------------------------|
| <mint-policy-name> | Enter a MiNT policy name to configure |
|--------------------|---------------------------------------|

---

### **Example**

```
RFController(config)#mint-policy global-default
RFController(config-mint-policy-global-default)#
```

---

### **NOTE**

For more information, see [Chapter 17, mint-policy](#).

---

## nac-list

### [Global Configuration Commands](#)

Configures a policy which configures a list of devices that can access a wireless controller managed network based on their MAC addresses.

| Command                  | Description                | Reference                |
|--------------------------|----------------------------|--------------------------|
| <a href="#">nac-list</a> | Creates a nac-list policy. | <a href="#">page 209</a> |

## nac-list

### *Global Configuration Commands*

Configures a network access control list that controls access to the wireless controller managed network.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
nac-list <NAC-LIST>
```

### Parameters

---

|                               |                                                 |
|-------------------------------|-------------------------------------------------|
| <code>&lt;NAC-LIST&gt;</code> | Enter the name of the nac-list to be configured |
|-------------------------------|-------------------------------------------------|

---

### Example

```
RFController(config)#nac test
RFController(config-nac-list-test)#?
NAC List Mode commands:
  exclude Specify MAC addresses to be excluded from the NAC enforcement list
  include Specify MAC addresses to be included in the NAC enforcement list
  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

RFController(config-nac-list-test)#
```

## nac-list mode

Table 11 Summarizes nac-list mode commands

**TABLE 11** nac-list mode commands

| Command        | Description                                                        | Reference                |
|----------------|--------------------------------------------------------------------|--------------------------|
| <i>exclude</i> | Specifies the MAC addresses excluded from the NAC enforcement list | <a href="#">page 211</a> |
| <i>include</i> | Specifies the MAC addresses included from the NAC enforcement list | <a href="#">page 212</a> |
| <i>no</i>      | Negates a command or sets its default values                       | <a href="#">page 213</a> |

***exclude****nac-list mode*

Specifies the MAC addresses to be excluded from the NAC enforcement list

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
exclude <Start-MAC> [<End-MAC> precedence <1-1000>|precedence <1-1000>]
```

**Parameters**


---

|                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>&lt;Start-MAC&gt; [&lt;End-MAC&gt; precedence &lt;1-1000&gt; precedence &lt;1-1000&gt;]</pre> | <p>Enter the starting MAC address of a range of MACs excluded from the NAC enforcement list</p> <ul style="list-style-type: none"> <li>• &lt;End-MAC&gt; – Enter the ending MAC address of a range of MACs. It is optional if a single mac address has to be added</li> <li>• precedence &lt;1-1000&gt; – Enter a rule precedence value from &lt;1-1000&gt;. The rules are verified in an increasing order of precedence</li> <li>• precedence &lt;1-1000&gt; – Enter a rule precedence value from &lt;1-1000&gt;. The rules are verified in an increasing order of precedence</li> </ul> |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-nac-list-test)#exclude 00-40-96-B0-BA-2A precedence 1
RFController(config-nac-list-test)#
```

## *include*

### *nac-list mode*

Specifies the MAC addresses included in the NAC enforcement list

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
include <Start-MAC> [<End-MAC> precedence <1-1000>|precedence <1-1000>]
```

### **Parameters**

---

|                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>&lt;Start-MAC&gt; [&lt;End-MAC&gt;<br/>precedence<br/>&lt;1-1000&gt; precedence<br/>&lt;1-1000&gt;]</p> | <p>Enter the starting MAC address of a range of MACs included in the NAC enforcement list</p> <ul style="list-style-type: none"> <li>• &lt;End-MAC&gt; – Enter the ending MAC address of a range of MACs. It is optional if a single MAC address has to be added</li> <li>• precedence &lt;1-1000&gt; – Enter a rule precedence value from &lt;1-1000&gt;. The rules are verified in an increasing order of precedence</li> <li>• precedence &lt;1-1000&gt; – Enter a rule precedence value from &lt;1-1000&gt;. The rules are verified in an increasing order of precedence</li> </ul> |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-nac-list-test)#include 00-40-96-B0-BA-2A precedence 1
RFController(config-nac-list-test)#
```

***no******nac-list mode***

Negates including or excluding a rule command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [exclude|include]
```

**Parameters**

|         |                                     |
|---------|-------------------------------------|
| exclude | Enter an exclude rule to be deleted |
| include | Enter an include rule to be deleted |

**Example**

```
RFController(config-nac-list-test)#no include 00-40-96-B0-BA-2A precedence 1
RFController(config-nac-list-test)#show context
nac-list test
RFController(config-nac-list-test)#
```

## no

### Global Configuration Commands

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no <parameter>
```

### Parameters

None

### Example

```
RFController(config)#no ?
aaa-policy          Delete a aaa policy
advanced-wips-policy Delete an advanced-wips policy
br650               Delete a br650 access point
br6511              Delete a br6511 access point
br6532              Delete a br6532 access point
br71xx              Delete a br71xx access point
association-acl-policy Delete an association-acl policy
auto-provisioning-policy Delete an auto-provisioning policy
captive-portal      Delete a captive portal
critical-resource-policy Remove device onboard critical resource policy
customize           Restore the custom cli commands to default
device              Delete multiple devices
device-categorization Delete device categorization object
dhcp-server-policy  DHCP server policy
dns-whitelist       Delete a whitelist object
event-system-policy Delete a event system policy
firewall-policy     Configure firewall policy
igmp-snoop-policy   Remove device onboard igmp snoop policy
ip                  Internet Protocol (IP)
mac                 MAC configuration
management-policy   Delete a management policy
nac-list            Delete an network access control list
password-encryption Disable password encryption in configuration
profile             Delete a profile and all its associated
                   configuration
radio-qos-policy    Delete a radio QoS configuration policy
radius-group        Local radius server group configuration
radius-server-policy Remove device onboard radius policy
radius-user-pool-policy Configure Radius User Pool
rf-domain           Delete one or more RF-domains and all their
                   associated configurations
```



|                 |                                                |
|-----------------|------------------------------------------------|
| rfs4000         | Delete an RFS4000 wireless controller          |
| rfs6000         | Delete an RFS6000 wireless controller          |
| rfs7000         | Delete an RFS7000 wireless controller          |
| role-policy     | Role based firewall policy                     |
| smart-rf-policy | Delete a smart-rf-policy                       |
| wips-policy     | Delete a wips policy                           |
| wlan            | Delete a wlan object                           |
| wlan-qos-policy | Delete a wireless lan QoS configuration policy |
| service         | Service Commands                               |

## password-encryption

### *Global Configuration Commands*

Enables password encryption with in a configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
password-encryption secret 2 <LINE>
```

### Parameters

---

|                 |                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| secret 2 <LINE> | Encrypts the passwords with secret phrase                                                                                                                                           |
|                 | <ul style="list-style-type: none"><li>• 2 - Specifies the type of encryption as either SHA256 or AES256</li><li>• &lt;LINE&gt; - Enter the passphrase used for encryption</li></ul> |

---

### Example

```
RFController(config)#password-encryption secret 2 brocade  
RFController(config)#
```

## profile

### *Global Configuration Commands*

Configures profile related commands. If no parameters are given, all the profiles are selected

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
profile{br650|br6511|br6532|br71xx|containing|filter|rfs4000|rfs6000|rfs7000}
profile containing <WORD> {filter} type [br6511|br6531|br71xx|rfs4000|
rfs6000|rfs7000]
profile filter type [br6511|br6531|br7131|rfs4000|rfs6000|rfs7000]
```

### Parameters

---

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{br650 br6511  br6532 br71xx  containing filter rfs4000  rfs6000 rfs7000}</pre> | <ul style="list-style-type: none"> <li>• containing &lt;WORD&gt; – Specifies the profiles that contain a sub-string in the host-name <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify a substring in the profile name to filter the profiles</li> </ul> </li> <li>• filter type – Specify the additional selection filter by profile type from the list of profiles <ul style="list-style-type: none"> <li>• br650 – Mobility 650 Access Point profile</li> <li>• br6511 – Mobility 6511 Access Point profile</li> <li>• br6532 – Mobility 6532 Access Point profile</li> <li>• br71xx – Mobility 7131 Series Access Point profile</li> <li>• rfs4000 – Mobility RFS4000 wireless controller profile</li> <li>• rfs6000 – Mobility RFS6000 wireless controller profile</li> <li>• rfs7000 – Mobility RFS7000 wireless controller profile</li> </ul> </li> </ul> |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Example

```

RFController(config-profile-default-rfs7000)#?
Profile Mode commands:
  aaa                               VPN AAA authentication settings
  ap-upgrade                         AP firmware upgrade
  arp                               Static Address Resolution Protocol (ARP)
  autoinstall                       Autoinstall Configuration commands
  automatic-write                   Enable automatic write of startup
                                   configuration file
  bridge                             Ethernet bridge
  cdp                               Cisco Discovery Protocol
  cluster                           Cluster configuration
  controller                        Add controller
  controller-group                  Controller group this controller belongs to
  crypto                            Encryption related commands
  dscp-mapping                      Configure IP DSCP to 802.1p priority mapping
                                   for untagged frames
  events                            System event messages
  interface                         Select an interface to configure
  ip                                Internet Protocol (IP)
  led                               Turn LEDs on/off on the device
  legacy-auto-update               Enable legacy device firmware auto update
  lldp                             Link Layer Discovery Protocol
  load-balancing                   Configure load balancing parameter
  local                             Local user authentication database for VPN
  logging                           Modify message logging facilities
  mac-address-table               MAC Address Table
  mint                             MiNT protocol
  misconfiguration-recovery-time   Check controller connectivity after
                                   configuration is received
  monitor                           Critical resource monitoring
  no                               Negate a command or set its defaults
  noc                               Configure the noc related setting
  ntp                               Ntp server A.B.C.D
  power-config                     Configure power mode
  preferred-controller-group       Controller group this system will prefer for
                                   adoption
  radius                           Configure device-level radius authentication
                                   parameters
  rf-domain-manager                RF Domain Manager
  spanning-tree                    Spanning tree
  use                               Set setting to use
  vpn                              Vpn configuration
  wep-shared-key-auth              Enable support for 802.11 WEP shared key
                                   authentication
  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

RFController(config-profile-default-rfs7000)#

```

---

## NOTE

For more information, see [Chapter 8, Profiles](#).

---

## radio-qos-policy

### *Global Configuration Commands*

Configures a radio quality of service policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
radio-qos-policy <radio-qos-policy-name>
```

### Parameters

---

|                         |                                  |
|-------------------------|----------------------------------|
| <radio-qos-policy-name> | Enter the name of the QoS policy |
|-------------------------|----------------------------------|

---

### Example

```
RFController(config)#radio-qos-policy test
RFController(config)#
```

---

### NOTE

For more information, see [Chapter 20, radio-qos-policy](#).

---

## radius-group

### *Global Configuration Commands*

Configures RADIUS user group parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
radius-group <radius-group-name>
```

### Parameters

---

|                     |                                             |
|---------------------|---------------------------------------------|
| <radius-group-name> | Enter a user group name up to 64 characters |
|---------------------|---------------------------------------------|

---

### Example

```
RFController(config)#radius-group testgroup  
RFController(config)#
```

---

### NOTE

For more information, see [Chapter 19, radius-policy](#).

---

## radius-server-policy

### *Global Configuration Commands*

Creates an onboard device RADIUS policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
radius-server-policy <radius-server-policy-name>
```

### **Parameters**

---

|                             |                                   |
|-----------------------------|-----------------------------------|
| <radius-server-policy-name> | Enter a RADIUS server policy name |
|-----------------------------|-----------------------------------|

---

### **Example**

```
RFController(config)#radius-server-policy testpolicy
RFController(config)#
```

---

### **NOTE**

For more information, see [Chapter 19, radius-policy](#).

---

## radius-user-pool-policy

### *Global Configuration Commands*

Configures a RADIUS user pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
radius-user-pool-policy <radius-user-pool-policy-name>
```

### **Parameters**

---

|                           |                                        |
|---------------------------|----------------------------------------|
| <radius-user-pool-policy> | Enter the radius-user-pool-policy name |
|---------------------------|----------------------------------------|

---

### **Example**

```
RFController(config)#radius-user-pool-policy testpool
RFController(config)#
```

---

### **NOTE**

For more information, see [Chapter 19, radius-policy](#).

---



## rf-domain

### [Global Configuration Commands](#)

RF Domain groups devices that can logically belong to one network. The rf-domain policy configures a set of parameters that enable devices to be configured quickly as belonging to a particular RF domain.

| Command                   | Description                 | Reference                |
|---------------------------|-----------------------------|--------------------------|
| <a href="#">rf-domain</a> | Creates a rf-domain policy. | <a href="#">page 224</a> |

## rf-domain

### *Global Configuration Commands*

Creates a RF-Domain configuration. If the policy does not exist, it creates a new policy.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
rf-domain {RF-DOMAIN|containing <WORD>}
```

### Parameters

---

|                               |                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {RF-DOMAIN containing <WORD>} | Defines the name of a RF-Domain <ul style="list-style-type: none"><li>• containing &lt;WORD&gt; - Specify domains that contain a sub-string in the domain name</li></ul> |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#rf-domain rfs7000
RFController(config)#
RFController(config-rf-domain-rfs7000)#

RFController(config)#rf-domain default
```

## rf-domain-mode

This section describes the default commands under rf-domain.

[Table 12](#) Summarizes rf-domain commands

**TABLE 12** rf-domain-mode

| Command                      | Description                                          | Reference                |
|------------------------------|------------------------------------------------------|--------------------------|
| <a href="#">channel-list</a> | Configures channel list advertised by radios         | <a href="#">page 226</a> |
| <a href="#">control-vlan</a> | Configures VLAN for traffic control on the RF Domain | <a href="#">page 227</a> |
| <a href="#">layout</a>       | Configures layout information                        | <a href="#">page 228</a> |

## *channel-list*

### *rf-domain-mode*

Configures channel list advertised by radios

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
channel-list [2.4GHz|5GHz|dynamic]
channel-list [2.4GHz|5GHz] <WORD>
```

### **Parameters**

---

|                       |                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [2.4GHz 5GHz dynamic] | <ul style="list-style-type: none"><li>• 2.4GHz &lt;WORD&gt; – Configures the channel list advertised by radios operating in 2.4GHz mode</li><li>• 5GHz &lt;WORD&gt; – Configures the channel list advertised by radios operating in 5GHz mode</li><li>• dynamic – Enables dynamic update of configured channel-list</li></ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-rf-domain-default)#channel-list 2.4GHz 1-10
RFController(config-rf-domain-default)#show context
rf-domain RFDOMAIN_UseCase1
location SanJose
contact txyr399@brocade.com
timezone America/Los_Angeles
country-code us
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
RFController(config-rf-domain-default)#
```

## *control-vlan*

### *rf-domain-mode*

Configures VLAN for traffic control on the RF Domain

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
control-vlan <1-4094>
```

### **Parameters**

---

|          |                                       |
|----------|---------------------------------------|
| <1-4094> | Configures VLAN ID between 1 and 4094 |
|----------|---------------------------------------|

---

### **Example**

```
RFController(config-rf-domain-default)#control-vlan 1
RFController(config-rf-domain-default)#show context
rf-domain RFDOMAIN_UseCase1
  location SanJose
  contact txyr399@brocade.com
  timezone America/Los_Angeles
  country-code us
  channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
  control-vlan 1
RFController(config-rf-domain-default)#
```

## *layout*

### *rf-domain-mode*

Configure layout maps for every rf-domain/floor/area. It allows users to place APs across the deployment map. A maximum of 256 layouts will be permitted.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
layout map-location <WORD> units [feet|meters] {area|floor} <WORD>
```

### **Parameters**

- 
- |                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>map-location &lt;WORD&gt; units<br/>[feet meters] [area  floor]<br/>&lt;WORD&gt;</pre> | <ul style="list-style-type: none"> <li>• map-location &lt;WORD&gt; – Configures map-location for the layout</li> <li>• &lt;WORD&gt; – Specify the URL to configure             <ul style="list-style-type: none"> <li>• units [feet meters] – Configures map units interms of feet/meters                 <ul style="list-style-type: none"> <li>• feet – Specify the measurement in feet</li> <li>• meters – Specify the measurement in meters</li> </ul> </li> <li>• {area &lt;WORD&gt; – Configures area name for the layout</li> <li>• floor &lt;WORD&gt; – Configures floor name for the layout</li> </ul> </li> </ul> |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

### **Example**

```
RFController(config-rf-domain-default)#layout map-location www.firstfloor.com
units meters area Ecospace floor Floor5
RFController(config-rf-domain-default)#

RFController(config-rf-domain-default)#show context
rf-domain default
country-code us
sensor-server 1 ip 172.16.10.14 port 1
channel-list dynamic
channel-list 2.4GHz 1,2,3,4,5,6,7,8,9,10
layout map-location www.firstfloor.com units meters area Ecospace floor
Floor5
RFController(config-rf-domain-default)#
```

### **NOTE**

The remaining commands under rf-domain are same as Device-Mode Commands. For more information, see [“Device specific commands”](#) on page 524.

## rfs4000

### *Global Configuration Commands*

Adds a Mobility RFS4000 Controller controller to the network

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
rfs4000 <DEVICE-RFS4000>
```

### **Parameters**

---

|                  |                                                        |
|------------------|--------------------------------------------------------|
| <DEVICE-RFS4000> | Enter the MAC address of a Mobility RFS4000 Controller |
|------------------|--------------------------------------------------------|

---

### **Example**

```
RFController(config)#rfs4000 10-20-30-40-50-60  
RFController(config-device-10-20-30-40-50-60)#
```

## rfs6000

### *Global Configuration Commands*

Adds a Mobility RFS6000 Controller controller to the network

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
rfs6000 <DEVICE-RFS6000>
```

### **Parameters**

---

|                  |                                                        |
|------------------|--------------------------------------------------------|
| <DEVICE-RFS6000> | Enter the MAC address of a Mobility RFS6000 Controller |
|------------------|--------------------------------------------------------|

---

### **Example**

```
RFController(config)#rfs6000 11-20-30-40-50-61  
RFController(config-device-11-20-30-40-50-61)#
```



## rfs7000

### [Global Configuration Commands](#)

Adds an Mobility RFS7000 Controller controller to the network

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
rfs7000 <DEVICE-RFS7000>
```

### Parameters

---

|                  |                                                        |
|------------------|--------------------------------------------------------|
| <DEVICE-RFS7000> | Enter the MAC address of a Mobility RFS7000 Controller |
|------------------|--------------------------------------------------------|

---

### Example

```
RFController(config)#rfs7000 12-20-30-40-50-62 ?  
RFController(config-device-12-20-30-40-50-62)#
```

## role-policy

### *Global Configuration Commands*

Configures a role based firewall policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
role-policy <role-policy-name>
```

### Parameters

---

|               |                                         |
|---------------|-----------------------------------------|
| <role-policy> | Enter the role-policy name to configure |
|---------------|-----------------------------------------|

---

### Example

```
RFController(config)#role-policy role1  
RFController(config)#
```

---

### NOTE

For more information, see [Chapter 21, role-policy](#).

---

## self

### *Global Configuration Commands*

Displays the configuration context of the currently logged device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
self
```

### **Parameters**

None

### **Example**

```
RFController(config)#self  
RFController(config-device-00-15-70-37-FA-BE)#
```

## service

### Global Configuration Commands

Retrieves system data (tables, log files, configuration, status and operation) for debugging and problem resolution

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
service [set|show cli]
service set [command-history <10-300>|reboot-history <10-100>|
upgrade-history <10-100>] {on <DEVICE-NAME>}
```

### Parameters

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set [ command-history <10-300> reboot-history <10-100> upgrade-history <10-100>] {on <DEVICE-NAME>} | Sets service parameters <ul style="list-style-type: none"> <li>• command-history &lt;10-300&gt; – Set the command history size between 10 and 300. The default size is 200</li> <li>• reboot-history &lt;10-100&gt; – Set the reboot history size between 10 and 100. The default size is 50</li> <li>• upgrade-history &lt;10-100&gt; – Set the upgrade history size between 10 and 100. The default size is 50               <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Optional. Displays the AP/Controller                   <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – AP/Controller name</li> </ul> </li> </ul> </li> </ul> |
| show cli                                                                                            | Displays running system information <ul style="list-style-type: none"> <li>• cli – Displays the CLI tree of current mode</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### Example

```
RFController(config)#service show cli
Global Config mode:
+-line
  +-console
    +-<0-0> [line console <0-0>]
  +-vty
    +-<0-871> [line vty <0-871> (<0-871>|)]
    +-<0-871> [line vty <0-871> (<0-871>|)]
+-help [help]
+-search
  +-WORD [help search WORD (|detailed|only-show|skip-show)]
  +-detailed [help search WORD (|detailed|only-show|skip-show)]
  +-only-show [help search WORD (|detailed|only-show|skip-show)]
  +-skip-show [help search WORD (|detailed|only-show|skip-show)]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
```

```

+-include-factory [show (running-config|session-config)
(|include-factory)]
+-interface [show running-config interface (|`WORD|ge <1-4>|me1|pc
<1-4>|vlan <1-4094>')] (|include-factory)]
+-WORD [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>')] (|include-factory)]
+-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan <1-4094>')] (|include-factory)]
+-ge
+-<1-4> [show running-config interface (|`WORD|ge <1-4>|me1|pc
<1-4>|vlan <1-4094>')] (|include-factory)]
+-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan <1-4094>')] (|include-factory)]
+-me1 [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>')] (|include-factory)]
+-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan
<1-4094>.....
RFController(config)#

RFController(config)#service set reboot-history 50
RFController(config)#

```

## show

### *Global Configuration Commands*

Displays running system information under various parameters such as, auto-provisioning-policy, advanced-wips policy and boot configuration details.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show <parameter>
```

### Parameters

None

---

### NOTE

For more information, see [Chapter 7, Show Commands](#).

---

### Example

```
RFController(config)#show ?
  adoption                Display information related to adoption to wireless
                          controller
  advanced-wips            Advanced WIPS
  ap-upgrade              AP Upgrade
  boot                    Display boot configuration.
  captive-portal          Captive portal commands
  cdp                     Cisco Discovery Protocol
  clock                   Display system clock
  cluster                 Cluster Protocol
  commands                Show command lists
  context                 Information about current context
  critical-resources      Critical Resources
  crypto                  Encryption related commands
  debug                   Debugging functions
  debugging               Debugging functions
  device-categorization  Device Categorization
  event-history           Display event history
  event-system-policy     Display event system policy
  file                    Display filesystem information
  firewall                Wireless Firewall
  interface               Interface Configuration/Statistics commands
  ip                      Internet Protocol (IP)
  ip-access-list-stats   IP Access list stats
  licenses                Show installed licenses and usage
  lldp                    Link Layer Discovery Protocol
  mac-access-list-stats  MAC Access list stats
```

|                     |                                            |
|---------------------|--------------------------------------------|
| mac-address-table   | Display MAC address table                  |
| mint                | MiNT protocol                              |
| noc                 | Noc-level information                      |
| ntp                 | Network time protocol                      |
| password-encryption | Pasword encryption                         |
| power               | Show power over ethernet command           |
| remote-debug        | Show details of remote debug sessions      |
| rf-domain-manager   | Show RF Domain Manager selection details   |
| role                | Role based firewall                        |
| running-config      | Current operating configuration            |
| session-changes     | Configuration changes made in this session |
| session-config      | This session configuration                 |
| sessions            | Display CLI sessions                       |
| smart-rf            | Smart-RF Management Commands               |
| spanning-tree       | Display spanning tree information          |
| startup-config      | Startup configuration                      |
| terminal            | Display terminal configuration parameters  |
| timezone            | The timezone                               |
| upgrade-status      | Display last image upgrade status          |
| version             | Display software & hardware version        |
| wireless            | Wireless commands                          |

RFController(config)#

## smart-rf-policy

### *Global Configuration Commands*

Configures a Smart-RF policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
smart-rf-policy <smart-rf-policy-name>
```

### **Parameters**

---

|                        |                                |
|------------------------|--------------------------------|
| <smart-rf-policy-name> | Enter the Smart-RF policy name |
|------------------------|--------------------------------|

---

### **Example**

```
RFController(config)#smart-rf-policy test
RFController(config-smart-rf-policy-test)#
```

---

### **NOTE**

For more information, see [Chapter 22, smart-rf-policy](#).

---



## wips-policy

### *Global Configuration Commands*

Configures a WIPS policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wips-policy <wips-policy-name>
```

### Parameters

---

|                    |                                         |
|--------------------|-----------------------------------------|
| <wips-policy-name> | Enter the WIPS policy name to configure |
|--------------------|-----------------------------------------|

---

### Example

```
RFController(config)#wips-policy test
RFController(config-wips-policy-test)#
```

---

### NOTE

For more information, see [Chapter 23, wips-policy](#).

---

## wlan

### [Global Configuration Commands](#)

Configures a wireless LAN.

| Command              | Description                | Reference                |
|----------------------|----------------------------|--------------------------|
| <a href="#">wlan</a> | Configures a wireless LAN. | <a href="#">page 224</a> |

## wlan

### *Global Configuration Commands*

Configures a WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wlan {[<WLAN>/containing <WORD>]}
```

### Parameters

---

|                          |                                                                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WLAN> containing <WORD> | Configures a wireless LAN <ul style="list-style-type: none"><li>• &lt;WLAN&gt; – Optional. Configures the WLAN specified by its WLAN number.</li><li>• containing &lt;WORD&gt; – Optional. Specify WLANs that contain a sub-string in the WLAN name</li></ul> |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#wlan 1
RFController(config-wlan-1)#

RFController(config)#wlan containing wlan1
RFController(config-wlan-{'containing': 'wlan1'})#
```

## wlan-mode commands

Configures WLAN related commands. Manual mapping of WLANs is erased when the actual WLAN is disabled and enabled immediately.

Use the (config) instance to configure WLAN related parameters.

To navigate to this instance, use the following commands:

```
RFController(config)#wlan <WLAN>
```

Table 13 Summarizes wlan-mode commands

**TABLE 13** wlan-mode commands

| Command                                     | Description                                                                    | Reference                |
|---------------------------------------------|--------------------------------------------------------------------------------|--------------------------|
| <a href="#">802.11k</a>                     | Configures support for 802.11k radio resource measurement                      | <a href="#">page 244</a> |
| <a href="#">802.11r</a>                     | Configures support for 802.11r fast BSS transition                             | <a href="#">page 245</a> |
| <a href="#">802.11w</a>                     | Enables support for Protected Management Frame (IEEE 802.11w) settings         | <a href="#">page 246</a> |
| <a href="#">accounting</a>                  | Defines the accounting configuration on this WLAN                              | <a href="#">page 247</a> |
| <a href="#">acl</a>                         | Defines the actions taken based on an ACL rule configuration                   | <a href="#">page 248</a> |
| <a href="#">answer-broadcast-probes</a>     | Allows the WLAN to respond to probes for broadcast ESS                         | <a href="#">page 249</a> |
| <a href="#">authentication-type</a>         | Sets the authentication type for the WLAN                                      | <a href="#">page 250</a> |
| <a href="#">bridging-mode</a>               | Sets the bridging mode                                                         | <a href="#">page 251</a> |
| <a href="#">broadcast-dhcp</a>              | Configures broadcast DHCP packet handling                                      | <a href="#">page 252</a> |
| <a href="#">broadcast-ssid</a>              | Advertises the SSID of the WLAN in beacons                                     | <a href="#">page 253</a> |
| <a href="#">captive-portal-enforcement</a>  | Configures the WLAN's captive-portal enforcement                               | <a href="#">page 254</a> |
| <a href="#">client-access</a>               | Enables WLAN client-access (normal data operations) on the WLAN                | <a href="#">page 255</a> |
| <a href="#">client-client-communication</a> | Allows the switching of frames from one wireless client to another on the WLAN | <a href="#">page 256</a> |
| <a href="#">client-load-balancing</a>       | Enables load balancing of the clients on the specified WLAN                    | <a href="#">page 257</a> |
| <a href="#">data-rates</a>                  | Specifies the 802.11 rates to be supported on the WLAN                         | <a href="#">page 258</a> |
| <a href="#">description</a>                 | Sets the WLAN's description                                                    | <a href="#">page 261</a> |
| <a href="#">encryption-type</a>             | Sets the encryption type for the WLAN                                          | <a href="#">page 262</a> |
| <a href="#">enforce-dhcp</a>                | Drops packets from clients with a static IP address                            | <a href="#">page 263</a> |
| <a href="#">ip</a>                          | Configures Internet Protocol (IP) settings                                     | <a href="#">page 264</a> |
| <a href="#">kerberos</a>                    | Configures Kerberos authentication parameters                                  | <a href="#">page 265</a> |
| <a href="#">motorola-extensions</a>         | Enables support for Motorola-specific extensions to 802.11                     | <a href="#">page 267</a> |
| <a href="#">no</a>                          | Negates a command or sets its default value                                    | <a href="#">page 268</a> |

**TABLE 13** wlan-mode commands

| <b>Command</b>          | <b>Description</b>                                              | <b>Reference</b>         |
|-------------------------|-----------------------------------------------------------------|--------------------------|
| <i>proxy-arp-mode</i>   | Enables proxy-arp-mode for ARP requests                         | <a href="#">page 269</a> |
| <i>radius</i>           | Configures the RADIUS related parameters                        | <a href="#">page 270</a> |
| <i>shutdown</i>         | Closes the WLAN                                                 | <a href="#">page 271</a> |
| <i>ssid</i>             | Configures the SSID the WLAN                                    | <a href="#">page 272</a> |
| <i>use</i>              | Sets the AAA policy configured for a WLAN                       | <a href="#">page 273</a> |
| <i>vlan</i>             | Sets the VLAN assignment for the WLAN                           | <a href="#">page 274</a> |
| <i>vlan-pool-member</i> | Adds a member VLAN to the pool of VLANs for the WLAN            | <a href="#">page 275</a> |
| <i>wep128</i>           | Configures WEP128 parameters                                    | <a href="#">page 276</a> |
| <i>wep64</i>            | Configures WEP64 parameters                                     | <a href="#">page 277</a> |
| <i>wireless-client</i>  | Configures the transmit power for wireless clients transmission | <a href="#">page 278</a> |
| <i>wlan</i>             | Modifies TKIP, CCMP (WPA/WPA2) related parameters               | <a href="#">page 241</a> |

## 802.11k

### wlan-mode commands

Configures support for 802.11k radio resource measurement

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
802.11k {channel-report}
```

### Parameters

---

|                  |                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------|
| {channel-report} | Optional. Configures support for radio resource measurement including the channel-report element in beacons and probe responses. |
|------------------|----------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wlan-1)#802.11k channel-report
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  802.11k channel-report
RFController(config-wlan-1)#
```

## 802.11r

### wlan-mode commands

Configures support for 802.11r fast BSS transition

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
802.11r {mobility-domain-id} <WORD>
```

### Parameters

---

|                             |                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| {mobility-domain-id} <WORD> | Configures the mobility domain ID for the roaming domain. A mobility domain ID must be 4 hexadecimal characters long. |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wlan-1)#802.11r mobility-domain-id 9f21
RFController(config-wlan-1)#
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  802.11r mobility-domain-id 9f21
```

## 802.11w

### wlan-mode commands

Enables support for Protected Management Frames (IEEE 802.11w) settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
802.11w [mandatory|optional|sa-query]
802.11w sa-query [attempts <1-15>|timeout <100-6000>]
```

### Parameters

---

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[mandatory optional sa-query]</p> | <ul style="list-style-type: none"> <li>• mandatory – Enforces protected management frame settings on the WLAN</li> <li>• optional – Advertises support for PMF but it is enforced only for clients that indicate their support</li> <li>• sa-query – Enables security association query settings             <ul style="list-style-type: none"> <li>• attempts &lt;1-15&gt; – Sets the number of times an sa-query message is attempted</li> <li>• timeout &lt;100-6000&gt; – Sets the timeout when waiting for a response to a security-association-query, before resending</li> </ul> </li> </ul> |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wlan-wlan1)#802.11w sa-query timeout 110
RFController(config-wlan-wlan1)#802.11w sa-query attempts 1
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  802.11r mobility-domain-id 9f21
  802.11w sa-query timeout 110
  802.11w sa-query attempts 1
```



## *accounting*

### *wlan-mode commands*

Defines the WLAN's accounting configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
accounting [radius|syslog host <WORD> {port} <1-65535>]
```

### **Parameters**

|                                     |                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radius                              | Uses RADIUS accounting on this WLAN                                                                                                                                                                                                                                                                                               |
| syslog host <WORD> {port} <1-65535> | Uses syslog accounting on this WLAN <ul style="list-style-type: none"> <li>• host - Enter a syslog destination hostname or IP address for accounting records</li> <li>• &lt;WORD&gt; - Enter the hostname or IP address</li> <li>• {port} &lt;1-65535&gt; - Enter a UDP port number for the syslog server from 1-65535</li> </ul> |

### **Example**

```
RFController(config-wlan-1)#accounting syslog host 172.16.10.12 port
RFController(config-wlan-1)#accounting syslog host 172.16.10.12 port 2
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  accounting syslog host 172.16.10.12 port 2
```

## *acl*

### *wlan-mode commands*

Defines the actions taken based on an ACL rule configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
acl exceed-rate wireless-client-denied-traffic <0-1000000> {blacklist
<0-86400>|disassociate}
```

### **Parameters**

---

|                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>exceed-rate<br/>         wireless-client-denied-traffic<br/>         &lt;0-1000000&gt; {blacklist<br/>         &lt;0-86400&gt;  disassociate}</p> | <p>Sets the actions taken based on an ACL rule configuration</p> <ul style="list-style-type: none"> <li>• exceed-rate – Action is taken when the rate exceeds a set value</li> <li>• wireless-client-traffic &lt;0-1000000&gt; – The action is to deny traffic to the client             <ul style="list-style-type: none"> <li>• &lt;0-1000000&gt; – Sets packet data</li> <li>• blacklist &lt;0-86400&gt; – Optional. Sets the time to blacklist a wireless client</li> <li>• disassociate – When enabled, a client is disassociated</li> </ul> </li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-1)#acl exceed-rate wireless-client-denied-traffic 20
disassociate
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  acl exceed-rate wireless-client-denied-traffic 20 disassociate
```

## *answer-broadcast-probes*

### *wlan-mode commands*

Allows the WLAN to respond to probe requests that do not specify an SSID.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
answer-broadcast-probes
```

### **Parameters**

None

### **Example**

```
RFController(config-wlan-1)#answer-broadcast-probes
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  answer-broadcast-probes
```

***authentication-type****wlan-mode commands*

Sets the authentication type for the WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
authentication-type [eap|eap-mac|eap-psk|kerberos|mac|none]
```

**Parameters**


---

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [eap eap-mac eap-psk kerberos mac none] | Sets the authentication type for this WLAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                         | <ul style="list-style-type: none"> <li>• eap – EAP authentication (802.1X)</li> <li>• eap-mac – EAP or MAC authentication depending on client (valid only with no encryption or WEP)</li> <li>• eap-psk – EAP authentication or pre-shared-keys depending on client (valid only with TKIP/CCMP)</li> <li>• kerberos – Kerberos authentication (encryption will change to WEP128 if its not already WEP128/Keyguard)</li> <li>• mac – MAC authentication (RADIUS lookup of MAC address)</li> <li>• none – No authentication is used</li> </ul> |

---

**Example**

```
authentication-type none
RFController(config-wlan-1)#authentication-type eap
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type eap
  authentication-type none
```

## *bridging-mode*

### *wlan-mode commands*

Configures how packets to/from this WLAN are bridged

#### **Syntax**

```
bridging-mode [local|tunnel]
```

#### **Parameters**

---

[local|tunnel]

- local - Packets are bridged between WLAN and local ethernet ports
  - tunnel - Packets are tunneled to other devices (typically wireless controllers)
- 

#### **Example**

```
RFController(config-wlan-1)#bridging-mode local
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode local
  encryption-type none
  authentication-type none
```

## ***broadcast-dhcp***

### *wlan-mode commands*

Configures broadcast DHCP packet handling

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
broadcast-dhcp validate-offer
```

### **Parameters**

---

|                |                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| validate-offer | Validates the broadcast DHCP packets which are destined to a wireless client associated to the radio before forwarding them over the air |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-1)#broadcast-dhcp validate-offer
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  broadcast-dhcp validate-offer
```

## ***broadcast-ssid***

### *wlan-mode commands*

Advertises the WLAN SSID in beacons

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
broadcast-ssid
```

### **Parameters**

None

### **Example**

```
RFController(config-wlan-1)#broadcast-ssid
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
```

## *captive-portal-enforcement*

### *wlan-mode commands*

Configures the WLAN's captive-portal enforcement

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
captive-portal-enforcement {fall-back}
```

### **Parameters**

---

|             |                                                                                            |
|-------------|--------------------------------------------------------------------------------------------|
| {fall-back} | Enforces captive-portal validation if WLAN authentication fails (applicable to EAP or MAC) |
|-------------|--------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-1)#captive-portal-enforcement fall-back
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  captive-portal-enforcement fall-back
```



## *client-access*

### *wlan-mode commands*

Enables WLAN client access (for normal data operations)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
client-access
```

### **Parameters**

None

### **Example**

```
RFController(config-wlan-wlan1)#client-access
```

### *client-client-communication*

#### *wlan-mode commands*

Allows the switching of frames from one wireless client to another

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
client-client-communication
```

#### **Parameters**

None

#### **Example**

```
RFController(config-wlan-wlan1)#client-client-communication
```

## *client-load-balancing*

### *wlan-mode commands*

Configures client load balancing of the clients on the specified WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
client-load-balancing {allow-single-band-clients [2.4ghz|5ghz]|
band-discovery-intvl <0-10000> |capability-ageout-time <0-10000>|
max-probe-req|probe-req-intvl}
client-load-balancing {max-probe-req|probe-req-intvl} [2.4ghz|5ghz] <0-1000>
```

### Parameters

---

|                                          |                                                                                                                                   |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| {allow-single-band-clients [2.4ghz 5ghz] | • allow-single-band-clients [2.4ghz 5ghz] – Allows single band wireless clients to associate even during load balancing           |
| band-discovery-intvl <0-10000>           | • 2.4ghz – Enables balancing of loads across 2.4ghz channels                                                                      |
| capability-ageout-time <0-10000>         | • 5ghz – Enables balancing of loads across 5ghz channels                                                                          |
| max-probe-req                            | • band-discovery-intvl <0-10000> – Configures time interval to discover client's band capability before associating it            |
| probe-req-intvl}                         | • capability-ageout-time <0-10000> – Configures time before it ages out client's capability information                           |
|                                          | • max-probe-req [2.4ghz 5ghz] <0-1000> – Configures client probe requests beyond which, it is allowed to associate                |
|                                          | • probe-req-intvl [2.4ghz 5ghz] <0-1000> – Configures interval for client probe requests beyond which, it is allowed to associate |
|                                          | • <0-1000> – Sets band discovery interval between 0 and 10000 seconds                                                             |

---

### Example

```
RFController(config-wlan-wlan1)#client-load-balancing
allow-single-band-clients 2.4ghz
RFController(config-wlan-wlan1)#

RFController(config-wlan-wlan1)#client-load-balancing band-discovery-intvl 2
RFController(config-wlan-wlan1)#

RFController(config-wlan-wlan1)#client-load-balancing probe-req-intvl 5ghz 5
RFController(config-wlan-wlan1)#
```

### *data-rates*

#### *wlan-mode commands*

Specifies the 802.11 rates supported on the WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
data-rates [2.4GHz|5GHz]
data-rates 2.4GHz [b-only|bg|bgn|custom|default|g-only|gn]
data-rates 5GHz [a-only|an|custom|default]
data-rates 5GHz custom [{12/18/24/36/48/54/9/basic-1/basi-11/
basic-12/basic-18/basic-2/basic-24/basic-36/basic-48/basic-5.5/basic-54/
basic-6/basic-9/basic-mcs0-7/mcs0-15/mcs0-7/mcs8-15}]
```

**Parameters**

|                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4Ghz [ b-only bg bgn<br> custom default g-only gn]                                                                                                                                                                                        | <p>Specifies the 802.11 rates supported on the WLAN when mapped to a 2.4GHz radio</p> <ul style="list-style-type: none"> <li>• b-only – Supports 11b-only mode</li> <li>• bg – Uses rates that support both 11b and 11g clients</li> <li>• bgn – Uses rates that support 11b, 11g and 11n clients</li> <li>• custom – Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is to be used as a basic rate (Eg: 'data-rates custom basic-1 basic-2 5.5 11')</li> <li>• default – Uses the rates configured on the radio</li> <li>• g-only – Uses rates that support operation in 11g-only mode</li> <li>• gn – Uses rates that support 11g and 11n clients</li> </ul>                                                                                                                                                                                                                                                 |
| 5GHz [a-only an <br>custom[[12 18 24 36 48 54<br> 9 basic-1 basi-11 <br>basic-12 basic-18 <br>basic-2 basic-24 <br>basic-36 basic-48 <br>basic-5.5 basic-54 <br>basic-6 basic-9 <br>basic-mcs0-7 <br>mcs0-15 mcs0-7 mcs8-15]]<br> default]] | <p>Specifies the 802.11 rates to be supported on the WLAN when mapped to a 5GHz radio</p> <ul style="list-style-type: none"> <li>• a-only – Uses rates that support operation in 11a-only mode</li> <li>• an – Uses rates that support 11a and 11n clients</li> <li>• default – Uses rates configured on the radio</li> <li>• custom [[12 18 24 36 48 54 9 basic-1 basi-11 basic-12 basic-18 basic-2 basic-24 basic-36 basic-48 basic-5.5 basic-54 basic-6 basic-9 basic-mcs0-7 mcs0-15 mcs0-7 mcs8-15]] – Configures a list of data rates by specifying each rate individually. Using 'basic-' as prefix before a rate, indicates it is used as a basic rate (Eg: 'data-rates custom basic-1 basic-2 5.5 11')</li> </ul>                                                                                                                                                                                                                                                             |
| {12 18 24 36 48 54 9 basic-1 basi-11 <br>basic-12 basic-18 <br>basic-2 basic-24 <br>basic-36 basic-48 <br>basic-5.5 basic-54 <br>basic-6 basic-9 <br>basic-mcs0-7 <br>mcs0-15 mcs0-7 mcs8-15]]<br> default]                                 | <ul style="list-style-type: none"> <li>• 12 – 12-Mbps</li> <li>• 18 – 18-Mbps</li> <li>• 24 – 24-Mbps</li> <li>• 36 – 36-Mbps</li> <li>• 48 – 48-Mbps</li> <li>• 54 – 54-Mbps</li> <li>• 6 – 6-Mbps</li> <li>• 9 – 9-Mbps</li> <li>• basic-1 – Basic 1-Mbps</li> <li>• basic-11 – Basic 11-Mbps</li> <li>• basic-12 – Basic 12-Mbps</li> <li>• basic-18 – Basic 18-Mbps</li> <li>• basic-2 – Basic 2-Mbps</li> <li>• basic-24 – Basic 24-Mbps</li> <li>• basic-36 – Basic 36-Mbps</li> <li>• basic-48 – Basic 48-Mbps</li> <li>• basic-5.5 – Basic 5.5-Mbps</li> <li>• basic-54 – Basic 54-Mbps</li> <li>• basic-6 – Basic 6-Mbps</li> <li>• basic-9 – Basic 9-Mbps</li> <li>• basic-mcs0-7 – Modulation and coding scheme 0-7 as a basic rate</li> <li>• mcs0-15 – Modulation and coding scheme 0-15</li> <li>• mcs0-7 – Modulation and coding scheme 0-7</li> <li>• mcs8-15 – Modulation and coding scheme 8-15</li> <li>• default – Uses rates configured on the radio]</li> </ul> |

**Example**

```
RFController(config-wlan-1)#data-rates 2.4 gn
RFController(config-wlan-1)#show context
```

## 5 Global Configuration Commands

```
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  data-rates 2.4GHz gn
  authentication-type none
```

## *description*

### *wlan-mode commands*

Defines the WLAN description. Used to identify the selected WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
description <LINE>
```

### **Parameters**

---

<LINE>

Defines the description for this WLAN. It is used to identify the selected WLAN.

---

### **Example**

```
RFController(config-wlan-1)#description testwlan
RFController(config-wlan-1)#show context
wlan 1
  description testwlan
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
```

## *encryption-type*

### *wlan-mode commands*

Sets the WLAN encryption type

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
encryption-type [ccmp|keyguard|none|tkip|tkip-ccmp|wep128|wep128-keyguard]
```

### **Parameters**

---

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>[ccmp keyguard none tkip tki<br/>p-ccmp wep128 <br/>wep128-keyguard]</pre> | <p>Sets the WLAN encryption type. Options include:</p> <ul style="list-style-type: none"> <li>• ccmp – AES Counter Mode CBC-MAC Protocol (AES-CCM CCMP)</li> <li>• keyguard – Keyguard-MCM (Mobile Computing Mode)</li> <li>• none – No encryption</li> <li>• tkip – Enables <i>Temporal Key Integrity Protocol</i> (TKIP)</li> <li>• tkip-ccmp – Enables both TKIP and CCMP on this WLAN</li> <li>• wep128 – Enables <i>Wired Equivalence Privacy</i> (WEP) with 128 bit keys</li> <li>• wep128-keyguard – Enables WEP128 as well as Keyguard-MCM on this WLAN</li> </ul> |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-wlan1)#encryption-type tkip-ccmp
RFController(config-wlan-wlan1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type tkip-ccmp
  authentication-type none
```



## *enforce-dhcp*

### *wlan-mode commands*

Drops the packets from clients with a static IP address

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
enforce-dhcp
```

### **Parameters**

None

### **Example**

```
RFController(config-wlan-1)#enforce-dhcp
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  enforce-dhcp
```

## *ip*

### *wlan-mode commands*

Configures Internet Protocol settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

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

### **Parameters**

---

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [arp dhcp] trust | Sets Internet Protocol settings for ARP and DHCP packets. <ul style="list-style-type: none"><li>• arp [header-mismatch-validation trust] – Address Resolution Protocol configuration<ul style="list-style-type: none"><li>• header-mismatch-validation– Verifies mismatch for source MAC in ARP header and ethernet header</li></ul></li><li>• dhcp trust – Dynamic Host Resolution Protocol configuration<ul style="list-style-type: none"><li>• trust – Sets the ARP/DHCP responses as trusted for this WLAN/range</li></ul></li></ul> |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-1)#ip dhcp trust
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  ip dhcp trust
```

## *kerberos*

### *wlan-mode commands*

Configures Kerberos authentication parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
kerberos [password|realm <WORD>|server]
kerberos password [0 <LINE>|2 <LINE>|<LINE>]
kerberos server [primary|secondary|timeout]
kerberos server primary host <IP> {port} <1-65535>
kerberos server secondary host <IP> {port} <1-65535>
kerberos server timeout <1-60>
```

### Parameters

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [password   realm   server | <ul style="list-style-type: none"> <li>• password [0 2 &lt;LINE&gt;] – Creates a KDC server password (up to 127 characters) <ul style="list-style-type: none"> <li>• 0 &lt;LINE&gt; – Enter the password</li> <li>• 2 &lt;LINE&gt; – Enter the password in encrypted form</li> <li>• &lt;LINE&gt; – The password</li> </ul> </li> <li>• realm &lt;WORD&gt; – Defines a KDC realm (up to 127 characters)</li> <li>• server [primary secondary timeout] – Modifies KDC server parameters <ul style="list-style-type: none"> <li>• primary host &lt;IP&gt; {port &lt;1-65535&gt;} – Defines the primary KDC server</li> <li>• secondary host &lt;IP&gt; {port &lt;1-65535&gt;} – Defines the secondary KDC server <ul style="list-style-type: none"> <li>• host – Enter the address of the KDC server</li> <li>• &lt;IP&gt; {port &lt;1-65535&gt;} – Sets the KDC server IP address <ul style="list-style-type: none"> <li>• port &lt;1-65535&gt; – Optional. Sets the KDC server authentication port in the range 1 to 65535. The default value is 88</li> </ul> </li> </ul> </li> <li>• timeout &lt;1-60&gt; – Modifies the KDC server's timeout parameters <ul style="list-style-type: none"> <li>• &lt;1-60&gt; – Defines the time the controller waits for a response from the KDC server before retrying</li> </ul> </li> </ul> </li> </ul> |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wlan-1)#kerberos server timeout 12
RFController(config-wlan-1)#

RFController(config-wlan-1)#kerberos server primary host 172.16.10.9 port 88
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
```

## 5 Global Configuration Commands

```
vlan 2  
bridging-mode tunnel  
encryption-type none  
authentication-type none  
kerberos server timeout 12  
kerberos server primary host 172.16.10.9
```

## *motorola-extensions*

### *wlan-mode commands*

Enables support for Motorola Solutions specific extensions to 802.11

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
motorola-extensions [move-command|smart-scan|symbol-load-information|
wmm-load-information]
```

### **Parameters**

---

|                         |                                                                                                                   |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|
| [move-command]          | • move-command – Enables support for Motorola-move (fast roaming)                                                 |
| smart-scan]             | • smart-scan – Enables support for smart scanning                                                                 |
| symbol-load-information | • symbol-load-information – Enables support for the Symbol Technologies load information element (Element ID 173) |
| wmm-load-information]   | • wmm-load-information – Enables support for the Motorola WMM load information element                            |

---

### **Example**

```
RFController(config-wlan-1)#motorola-extensions wmm-load-information
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  motorola-extensions wmm-load-information
```

### ***no***

#### *wlan-mode commands*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
no <parameter>
```

#### **Parameters**

None

#### **Usage Guidelines**

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

#### **Example**

```
RFController(config-wlan-wlan1)#no wep64 key 1
RFController(config-wlan-wlan1)#

RFController(config-wlan-wlan1)#no ip arp trust
RFController(config-wlan-wlan1)#
```

## *proxy-arp-mode*

### *wlan-mode commands*

Enables proxy-arp mode for handling ARP requests

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
proxy-arp-mode [dynamic|strict]
```

### **Parameters**

---

|                  |                                                                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [dynamic strict] | <ul style="list-style-type: none"><li>• dynamic – Forwards ARP requests to the wireless side (for which a response could not be proxied)</li><li>• strict – Does not forward ARP requests to the wireless side</li></ul> |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-1)#proxy-arp-mode strict
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  proxy-arp-mode strict
```

***radius***

*wlan-mode commands*

Configures RADIUS related parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
radius [dynamic-authorization|nas-identifier <WORD>|nas-port-id
<WORD>|vlan-assignment]
```

**Parameters**

|                       |                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------|
| dynamic-authorization | Enables support for disconnect and change-of-authorization messages (RFC5176)       |
| nas-identifier <WORD> | The WLAN NAS identifier sent to the RADIUS server. Maximum length is 256 characters |
| nas-port-id <port>    | The WLAN NAS-port-id sent to the RADIUS server. Maximum length is 256 characters    |
| vlan-assignment       | Sets the VLAN assignment of this WLAN                                               |

**Example**

```
RFController(config-wlan-1)#radius vlan-assignment
RFController(config-wlan-1)#show context
wlan 1
  ssid WLAN_USECASE_01
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  radius vlan-assignment
```



## ***shutdown***

### *wlan-mode commands*

Closes the WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
shutdown
```

### **Parameters**

None

### **Example**

```
RFController(config-wlan-1)#shutdown
```

## *ssid*

### *wlan-mode commands*

Configures the SSID for the WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
ssid <WORD>
```

### **Parameters**

---

|        |                                                          |
|--------|----------------------------------------------------------|
| <WORD> | Enter the SSID of this WLAN. <ssid> up to 32 characters. |
|--------|----------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-1)#ssid Test1
RFController(config-wlan-1)#show context
wlan 1
  ssid Test1
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
```

**use****wlan-mode commands**

Sets the AAA policy configured for a WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
use [aaa-policy
<aaa-policy-name>|association-acl-policy<association-policy-name>|captive-portal
<captive-portal-name>|ip-access-list
<ip-access-list-name>|mac-access-list <mac-access-list-name>|wlan-qos-policy
<wlan-qos-policy-name>]

use ip-access-list [in|out] <ip-access-list-name>
use mac-access-list [in|out] <mac-access-list-name>
```

**Parameters**

|                                                     |                                                                                                                                                                                                                          |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aaa-policy <aaa-policy-name>                        | Uses the aaa policy for the WLAN <ul style="list-style-type: none"> <li>• &lt;aaa-policy-name&gt; - Enter the aaa-policy to use</li> </ul>                                                                               |
| association-acl<br><association-policy-name>        | Uses the association-acl policy for the WLAN <ul style="list-style-type: none"> <li>• &lt;association-policy-name&gt; - Enter the association-policy to use</li> </ul>                                                   |
| captive-portal<br><captive-portal-name>             | Enables the WLAN's captive-portal authentication                                                                                                                                                                         |
| ip-access-list [in  out]<br><ip-access-list-name>   | Specifies the ip-access-list used <ul style="list-style-type: none"> <li>• in - Incoming packets</li> <li>• out - Outgoing packets</li> <li>• &lt;ip-access-list-name&gt; - Enter the ip-access-list to use</li> </ul>   |
| mac-access-list [in  out]<br><mac-access-list-name> | Specifies the mac-access-list used <ul style="list-style-type: none"> <li>• in - Incoming packets</li> <li>• out - Outgoing packets</li> <li>• &lt;ip-access-list-name&gt; - Enter the mac-access-list to use</li> </ul> |
| wlan-qos-policy<br><wlan-qos-policy-name>           | Uses the wlan-qos-policy for the WLAN <ul style="list-style-type: none"> <li>• &lt;wlan-qos-policy-name&gt; - Enter the wlan-qos-policy to use</li> </ul>                                                                |

**Example**

```
RFController(config-wlan-1)#use ip-access-list in brocade
RFController(config-wlan-1)#
```

## *vlan*

### *wlan-mode commands*

Sets the VLAN assignment of the WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
vlan <1-4094>
```

### **Parameters**

---

|          |                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------|
| <1-4094> | Sets the WLAN's VLAN. This command starts a new VLAN assignment for a WLAN index. All prior VLAN settings are erased. |
|----------|-----------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-wlan-wlan1)#vlan 4
RFController(config-wlan-wlan1)#

RFController(config-wlan-wlan1)#show interface vlan 4
Interface vlan4 is UP
  Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
  Index: 5, Metric: 1, MTU: 1500
  IP-Address: 157.235.208.252/24
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

RFController(config-wlan-wlan1)#
```

## *vlan-pool-member*

### *wlan-mode commands*

Add a member vlan to the pool of VLANs for the WLAN

---

**NOTE**

Configuration of a VLAN pool overrides the 'vlan' configuration. Supported in the following platforms:

---

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
vlan-pool-member <WORD> {limit} <0-8192>
```

**Parameters**


---

|                                                  |                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;WORD&gt; {limit} &lt;0-8192&gt;</code> | Defines the VLAN configuration. It can be either a single index, or a list (1,3,7) <ul style="list-style-type: none"> <li>• <code>limit &lt;0 -8192&gt;</code> – Optional. It can be ignored if the number of clients are limited and expected to be well within the limits of the DHCP pool on the vlan.</li> <li>• <code>&lt;0-8192&gt;</code> – Specifies the number of users allowed</li> </ul> |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-wlan-1)#vlan-pool-member 1-10 limit 1
RFController(config-wlan-1)#show context
wlan 1
  ssid Test1
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  vlan-pool-member 1 limit 1
  vlan-pool-member 2 limit 1
  vlan-pool-member 3 limit 1
  vlan-pool-member 4 limit 1
  vlan-pool-member 5 limit 1
  vlan-pool-member 6 limit 1
  vlan-pool-member 7 limit 1
  vlan-pool-member 8 limit 1
  vlan-pool-member 9 limit 1
  vlan-pool-member 10 limit 1
  vlan-pool-member 11 limit 1
  vlan-pool-member 12 limit 1
  vlan-pool-member 13 limit 1
  vlan-pool-member 14 limit 1
  vlan-pool-member 15 limit 1
  vlan-pool-member 16 limit 1
```

## wep128

### wlan-mode commands

Configures WEP128 parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wep128 [key|keys-from-passkey|transmit-key]
wep128 key <1-4> [ascii|hex] [0|2|<WORD>]
wep128 keys-from-passkey <WORD>
wep128 transmit-key <1-4>
```

### Parameters

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key <1-4> [ascii hex]<br>[0 2 <WORD>] | key <1-4> [ascii hex] – Configures pre-shared hex keys <ul style="list-style-type: none"> <li>• ascii [0 2 &lt;WORD&gt;] – Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128) <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Keys as 13 ascii characters that are converted to hex, or 26 hexadecimal characters or as a 64 characters hexadecimal value if encrypted</li> </ul> </li> <li>• hex [0 2 &lt;WORD&gt;] – Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) <ul style="list-style-type: none"> <li>• 0 – Enter a clear text key</li> <li>• 2 – Enter an encrypted key</li> <li>• &lt;WORD&gt; – Keys as 13 ascii characters that are converted to hex, or 26 hexadecimal characters</li> </ul> </li> </ul> |
| keys-from-passkey <WORD>              | Specifies a passphrase from which keys are derived <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Sets the passphrase (between 4 and 32 characters)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| transmit-key <1-4>                    | Defines the key index used for transmission from an AP to a client                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### Example

```
RFController(config-wlan-1)#wep128 transmit-key 1
RFController(config-wlan-1)#
```

## wep64

### wlan-mode commands

Configures WEP64 parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wep64 [key|keys-from-passkey|transmit-key]
wep64 key <1-4> [ascii|hex] [0|2|<WORD>]
wep64 keys-from-passkey <WORD>
wep64 transmit-key <1-4>]
```

### Parameters

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| key <1-4> [ascii hex]<br>[0 2 <WORD>] | key <1-4> [ascii hex] – Configures pre-shared hex keys <ul style="list-style-type: none"> <li>• ascii [0 2 &lt;WORD&gt;] – Sets keys as ASCII characters (5 characters for WEP64, 13 for WEP128)</li> <li>• hex [0 2 &lt;WORD&gt;] – Sets keys as hexadecimal characters (10 characters for WEP64, 26 for WEP128) <ul style="list-style-type: none"> <li>• 0 – Enter a clear text key</li> <li>• 2 – Enter an encrypted key</li> <li>• &lt;WORD&gt; – Key (10 hex or 5 ASCII characters for WEP64, 26 hex or 13 ASCII characters for WEP128)</li> </ul> </li> </ul> |
| keys-from-passkey <WORD>              | Specifies a passphrase from which keys are derived <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Sets the passphrase (between 4 and 32 characters)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                             |
| transmit-key <1-4>                    | Defines the key index used for transmission from an AP to client                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

### Example

```
RFController(config-wlan-1)#wep64 key 1 ascii symbo

RFController(config-wlan-1)#wep64 transmit-key 1
RFController(config-wlan-1)#
```

## wireless-client

### wlan-mode commands

Configures the transmit power indicated to wireless clients for transmission

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wireless-client [cred-cache-ageout <60-86400>|hold-time <1-300>
|inactivity-timeout <60-86400>|max-firewall-sessions <10-10000>|
reauthentication <30-86400>|tx-power <0-20>|vlan-cache-out <60-86400>]
```

### Parameters

|                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>cred-cache-ageout &lt;60-86400&gt; hold-time &lt;1-300&gt;  inactivity-timeout &lt;60-86400&gt; max-firewall-sessi ons &lt;10-10000&gt;  reauthentication &lt;30-86400&gt; tx-power &lt;0-20&gt; vlan-cache-out &lt;60-86400&gt;</pre> | <ul style="list-style-type: none"> <li>• cred-cache-ageout &lt;60-86400&gt; – Configures the timeout for which the client credentials such as encryption keys are cached across associations <ul style="list-style-type: none"> <li>• &lt;60-86400&gt; – Specify the timeout between 60 and 86400 seconds</li> </ul> </li> <li>• hold-time &lt;1-300&gt; – Time for which wireless client state information is cached post roaming <ul style="list-style-type: none"> <li>• &lt;1-300&gt; – Specify the hold time between 1 and 300 seconds</li> </ul> </li> <li>• inactivity-timeout &lt;60-86400&gt; – Specifies inactivity timeout in seconds. If a frame is not received from a wireless client for this amount of time, the client is disassociated</li> <li>• max-firewall-sessions &lt;10-10000&gt; – Specifies the maximum firewall sessions allowed per wireless client on the wlan <ul style="list-style-type: none"> <li>• &lt;10-10000&gt; – Specify the maximum number of firewall sessions allowed between 10 and 10000</li> </ul> </li> <li>• reauthentication &lt;30-86400&gt; – Configures periodic reauthentication of associated clients <ul style="list-style-type: none"> <li>• &lt;30-86400&gt; – Sets the reauthentication time period between 30 and 86400 seconds</li> </ul> </li> <li>• tx-power &lt;0-20&gt; – Configures the transmit power indicated to wireless clients for transmission <ul style="list-style-type: none"> <li>• &lt;0-20&gt; – Sets the transmit power in dBm</li> </ul> </li> <li>• vlan-cache-ageout &lt;60-86400&gt; – Configures the timeout for which client VLAN information is cached across associations <ul style="list-style-type: none"> <li>• &lt;60-86400&gt; – Sets the timeout between 60 and 86400 seconds</li> </ul> </li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



**Example**

```
RFController(config-wlan-1)#wireless-client cred-cache-ageout 65

RFController(config-wlan-1)#wireless-client hold-time 10

RFController(config-wlan-1)#wireless-client max-firewall-sessions 100

RFController(config-wlan-1)#wireless-client reauthentication 35

RFController(config-wlan-1)#wireless-client tx-power 12
RFController(config-wlan-1)#show context
wlan 1
  ssid Test1
  vlan 2
  bridging-mode tunnel
  encryption-type none
  authentication-type none
  wireless-client cred-cache-ageout 65
  wireless-client hold-time 10
  wireless-client max-firewall-sessions 100
  wireless-client reauthentication 35
  wireless-client tx-power 12
```

### *wpa-wpa2*

#### *wlan-mode commands*

Modifies TKIP-CCMP (WPA/WPA2) related parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
wpa-wpa2 [exclude-wpa2-tkip|handshake|key-rotation|opp-pmk-caching|
pmk-caching|preauthentication|psk|tkip-countermeasures]
wpa-wpa2 handshake [attempts <1-5>|init-wait <5-1000000>|priority
[high_|normal|]|timeout <10-5000>]
wpa-wpa2 key-rotation [broadcast|unicast] <30-86400>
wpa-wpa2 psk [0|2|<LINE>] <LINE>
wpa-wpa2 tkip-countermeasures holdtime <0-65535>]
```

**Parameters**

|                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>exclude-wpa2-tkip</code>                                                                                   | Excludes the WPA2 version of TKIP, support only WPA-TKIP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>handshake [attempts &lt;1-5&gt;   init-wait &lt;5-1000000&gt;   priority   timeout &lt;10-5000&gt;]</code> | Configures the parameters related to the WPA/WPA2 handshake <ul style="list-style-type: none"> <li>attempts &lt;1-5&gt; – Configures the total number of times a message is transmitted towards a non-responsive client</li> <li>init-wait &lt;5-1000000&gt; – Configure a wait-time before the first message of the handshake is transmitted from the AP</li> <li>priority [high   normal] – Configure the relative priority of the handshake messages compared to other data traffic <ul style="list-style-type: none"> <li>high – Treats handshake messages as high priority packets in the radio</li> <li>normal – Treats handshake messages as normal priority packets in the radio</li> </ul> </li> <li>timeout &lt;10-5000&gt; – Configures the timeout for a handshake message, before it is retried</li> </ul> |
| <code>key-rotation [broadcast   unicast] &lt;30-86400&gt;</code>                                                 | Configures parameters related to periodic rotation of encryption keys <ul style="list-style-type: none"> <li>broadcast – Sets the rotation of keys used for broadcast and multicast traffic</li> <li>unicast – Sets the rotation of keys used for unicast traffic <ul style="list-style-type: none"> <li>&lt;30-86400&gt; – Specify the time in seconds when the keys are rotated</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>opp-pmk-caching</code>                                                                                     | Enables the use of opportunistic key caching (same PMK across APs for fast roaming with EAP.802.1x)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>pmk-caching</code>                                                                                         | Enables the use of cached pairwise master keys (fast roaming with eap/802.1x)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>preauthentication</code>                                                                                   | Enables preauthentication usage (WPA2 fast roaming)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>psk[0 2 &lt;LINE&gt;] &lt;LINE&gt;</code>                                                                  | <ul style="list-style-type: none"> <li>psk – Configures a pre-shared key</li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>0 – Enter a clear text key</li> <li>2 – Enter an encrypted key</li> <li>&lt;LINE&gt; – Enter pre-shared key either as a passphrase between 8 and 63 characters long, or as a 64 character (256bit) hexadecimal value <ul style="list-style-type: none"> <li>&lt;LINE&gt; – Enter pre-shared key either as a passphrase between 8 and 63 characters long, or as a 64 character (256bit) hexadecimal value</li> </ul> </li> </ul>                                                                                                                                                                                                    |
| <code>tkip-countermeasures holdtime &lt;0-65535&gt;</code>                                                       | Configures TKIP countermeasures related parameters <ul style="list-style-type: none"> <li>&lt;holdtime &lt;0-65535&gt; – Configures the amount of time a WLAN is disabled when TKIP counter measures are invoked</li> <li>&lt;0-65535&gt; – Enter the hold-time in seconds</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Example**

```
RFController(config-wlan-wlan1)#wpa-wpa2 tkip-countermeasures hold-time 2
RFController(config-wlan-1)#show context
wlan 1
  ssid Test1
  vlan 2
```

## wlan-qos-policy

### *Global Configuration Commands*

Configures a WLAN QoS policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
wlan-qos-policy <wlan-qos-policy-name>
```

### **Parameters**

---

|                        |                                           |
|------------------------|-------------------------------------------|
| <wlan-qos-policy-name> | Enter a WLAN QoS-policy name to configure |
|------------------------|-------------------------------------------|

---

### **Example**

```
RFController(config)#wlan-qos-policy test
RFController(config-wlan-qos-test)#
```

---

### **NOTE**

For more information, see [Chapter 24, wlan-qos-policy](#).

---

## write

### *Global Configuration Commands*

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
write [terminal|memory]
```

### Parameters

|          |                         |
|----------|-------------------------|
| memory   | Writes to the NV memory |
| terminal | Writes to terminal      |

### Example

```
RFController#write memory
[OK]
RFController#
```

```
RFController#write terminal
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
  enable
  calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
  voice-prioritization
  svp-prioritization
  wmm background cw-max 8
  wmm video txop-limit 9
.....RFC
ontroller>
```

## 5 Global Configuration Commands

# Common Commands

---

## In this chapter

- [Common Commands](#) ..... 285

This chapter describes the CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes.

The PRIV EXEC command set contains commands available within the USER EXEC mode. Some commands can be entered in either mode. Commands entered in either the USER EXEC mode or the PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

## Common Commands

[Table 14](#) Summarizes Common Commands

**TABLE 14** Common Commands

| Command                 | Description                                                   | Reference                |
|-------------------------|---------------------------------------------------------------|--------------------------|
| <a href="#">clear</a>   | Clears the display screen                                     | <a href="#">page 286</a> |
| <a href="#">commit</a>  | Commits all changes made in the active session                | <a href="#">page 287</a> |
| <a href="#">exit</a>    | Ends the current mode and moves to the previous mode          | <a href="#">page 288</a> |
| <a href="#">help</a>    | Displays the interactive help system                          | <a href="#">page 289</a> |
| <a href="#">no</a>      | Negates a command or sets its defaults                        | <a href="#">page 293</a> |
| <a href="#">show</a>    | Shows running system information                              | <a href="#">page 295</a> |
| <a href="#">revert</a>  | Reverts the changes made to their last saved configuration    | <a href="#">page 297</a> |
| <a href="#">service</a> | Services or debugs the controller                             | <a href="#">page 298</a> |
| <a href="#">write</a>   | Writes the system running configuration to memory or terminal | <a href="#">page 317</a> |

### clrscr

#### *Common Commands*

Clears the screen and refreshes the prompt (#)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
clrscr
```

#### **Parameters**

None

#### **Example**

```
RFController>clrscr  
RFController>
```



## commit

### *Common Commands*

Commits all changes made in the active session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
commit {write}{memory}
```

### Parameters

|        |                                                              |
|--------|--------------------------------------------------------------|
| write  | If a commit succeeds, the configuration is written to memory |
| memory | Writes to memory                                             |

### Example

```
RFController>commit write memory  
[OK]  
RFController>
```

### exit

#### *Common Commands*

Ends the current mode and moves to the previous mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
exit
```

#### **Parameters**

None

#### **Example**

```
RFController(config)#exit  
RFController#
```

## help

### Common Commands

Describes the interactive help system.

Use this command to access the advanced help feature. Use “?” anytime at the command prompt to access the help topic.

Two kinds of help are provided:

- Full help is available when ready to enter a command argument
- Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example 'show ve?').

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
help {show configuration-tree/search}
help search <WORD> {detailed/only-show/skip-show/skip-no}
```

### Parameters

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| show configuration-tree                             | Displays running system information <ul style="list-style-type: none"> <li>• configuration-tree – Displays the relationships amongst configuration objects</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| search <WORD><br>{detailed only-show <br>skip-show} | Searches for CLI commands related to a specific term <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter a target term for a search (Eg: a feature or a configuration parameter)               <ul style="list-style-type: none"> <li>• detailed – Searches and displays help strings in addition to mode and commands</li> <li>• only-show – Displays only "show" commands, not configuration commands</li> <li>• skip-show – Displays only configuration commands, not "show" commands</li> <li>• skip-no – Displays only configuration commands, not 'no' commands</li> </ul> </li> </ul> |

## Example

```
RFController>help search crypto detailed
Found 29 references for "crypto"
    Found 113 references for "crypto"

Mode      : User Exec
Command : show crypto key rsa (|public-key-detail) (|(on DEVICE-NAME))
          \ Show running system information
          \ Encryption related commands
          \ Key management operations
          \ Show RSA public Keys
          \ Show the public key in PEM format
          \ On AP/Controller
          \ AP / Controller name

: show crypto pki trustpoints (WORD|all|)(|(on DEVICE-NAME))
  \ Show running system information
  \ Encryption related commands
  \ Public Key Infrastructure related commands
  \ Display the configured trustpoints
  \ Display a particular trustpoint's details
  \ Display details for all trustpoints
  \ On AP/Controller
  \ AP / Controller name

: show crypto isakmp sa (|(on DEVICE-NAME))
  \ Show running system information
  \ Encryption Module
  \ Show ISAKMP related statistics
  \ Show all ISAKMP Security Associations
  \ On AP/Controller
  \ AP / Controller name

: show crypto ipsec sa (|(on DEVICE-NAME))
  \ Show running system information
  \ Encryption Module
  \ Show IPSec related statistics
  \ IPSec security association
  \ On AP/Controller
  \ AP / Controller name

: crypto key generate rsa WORD <1024-2048> (|(on DEVICE-NAME))
  \ Encryption related commands
  \ Key management operations
  \ Generate a keypair
  \ Generate a RSA keypair
  \ Keypair name
```

RFController>

```
RFController>help show configuration-tree
```

```
## ACCESS-POINT / SWITCH ## ----+
|
+--> [[ RF-DOMAIN ]]
|
+--> [[ PROFILE ]]
|
```

```

                                +--> Device specific parameters (license, serial
number, hostname)
                                |
                                +--> Configuration Overrides of rf-domain and
profile

## RF-DOMAIN ## ---+
|
|   +--> RF parameters, WIPS server parameters
|   |
|   +--> [[ SMART-RF-POLICY ]]
|   |
|   +--> [[ WIPS POLICY ]]

## PROFILE ## ---+
|
|   +--> Physical interface (interface GE,ME,UP etc)
|   |
|   |   +--> [[ RATE-LIMIT-TRUST-POLICY ]]
|   |
|   +--> Vlan interface (interface VLAN1/VLAN36 etc)
|   |
|   +--> Radio interface (interface RADIO1, RADIO2 etc)
|   |
|   |   +--> Radio specific Configuration
|   |   |
|   |   +--> [[ RADIO-QOS-POLICY ]]
|   |   |
|   |   +--> [[ ASSOC-ACL-POLICY ]]
|   |   |
|   |   +--> [[ WLAN ]]
|   |
|   +--> [[ MANAGEMENT-POLICY ]]
|   |
|   +--> [[ DHCP-SERVER-POLICY ]]
|   |
|   +--> [[ FIREWALL-POLICY ]]
|   |
|   +--> [[ NAT-POLICY ]]

.....
RFController>

RFController>help search clrscr only-show
found no commands containing "clrscr"
RFController>

RFController>help search service skip-show
Found 32 references for "service"

Mode      : User Exec
Command   : service show cli
           : service show rim config (|include-factory)
           : service show wireless credential-cache
           : service show wireless neighbors
           : service show general stats(|(on DEVICE-OR-DOMAIN-NAME))
           : service show process(|(on DEVICE-OR-DOMAIN-NAME))
           : service show mem(|(on DEVICE-OR-DOMAIN-NAME))
           : service show top(|(on DEVICE-OR-DOMAIN-NAME))
           : service show crash-info (|(on DEVICE-OR-DOMAIN-NAME))

```

## 6 Common Commands

```
      : service cli-tables-skin
(none|minimal|thin|thick|stars|hashes|percent|ansi|utf-8) (grid|)
      : service cli-tables-expand (|left|right)
      : service wireless clear unauthorized aps (|(on DEVICE-OR-DOMAIN-NAME))
      : service wireless qos delete-ts-spec AA-BB-CC-DD-EE-FF tid <0-7>
      : service wireless wips clear-event-history
      : service wireless wips clear-mu-blacklist (all|(mac
AA-BB-CC-DD-EE-FF))
      : service radio <1-3> dfs simulate-radar (primary|extension)
      : service smart-rf run-calibration
      : service smart-rf stop-calibration
      : service cluster manual-revert
      : service advanced-wips clear-event-history
      : service advanced-wips clear-event-history
(dos-eap-failure-spoof|id-theft-out-of-sequence|id-theft-eapol-success-spoof-
detected|wlan-jack-attack-detected|ssid-jack-attack-detected|monkey-jack-att
ack-detected|null-probe-response-detected|fata-jack-detected|fake-dhcp-server
-detected|crackable-wep-iv-used|windows-zero-config-memory-leak|multicast-all
-systems-on-subnet|multicast-all-routers-on-subnet|multicast-ospf-all-routers
-detection|multicast-ospf-designated-routers-detection|multicast-rip2-routers
-detection|multicast-igmp-routers-detection|multicast-vrrp-agent|multicast-hs
rp-agent|multicast-dhcp-server-relay-agent|multicast-igmp-detection|netbios-d
etection|stp-detection|ipx-detection|invalid-management-frame|invalid-channel
-advertized|dos-deauthentication-detection|dos-disassociation-detection|dos-r
ts-flood|rogue-ap-detection|accidental-association|probe-response-flood|dos-c
ts-flood|dos-eapol-logoff-storm|unauthorized-bridge)
      : service start-shell
      : service pktcap on(bridge|drop|deny|router|wireless|vpn|radio
(all|<1-3>))(|promiscuous)|rim|interface `WORD`ge <1-4>|me1|pc <1-4>|vlan
<1-4094>')(|{direction (any|inbound|outbound)|acl-name WORD|verbose|hex|count
<1-1000000>|snap <1-2048>|write (FILE|URL|tzsp WORD)|tcpdump})(|filter LINE)

Mode      : Profile Mode
Command   : service watchdog

Mode      : Radio Mode
Command   : service antenna-type
(default|dual-band|omni|yagi|embedded|panel|patch|sector|out-omni|in-patch|br
650-int)
      : service disable-erp
      : service disable-ht-protection
      : service recalibration-interval <0-65535>
.....RFC
ontroller>

RFController>help search mint only-show
Found 8 references for "mint"

Mode      : User Exec
Command   : show mint neighbors (|details)(|(on DEVICE-NAME))
      : show mint links (|details)(|(on DEVICE-NAME))
      : show mint id(|(on DEVICE-NAME))
      : show mint stats(|(on DEVICE-NAME))
      : show mint route(|(on DEVICE-NAME))
      : show mint lsp
      : show mint lsp-db (|details)(|(on DEVICE-NAME))
      : show mint mlcp(|(on DEVICE-NAME))
RFController>
```

**no***Common Commands*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no <parameter>
```

**Parameters**

None

**Example**

```
RFController#no ?
  adoption      Reset adoption state of the device (& all devices adopted to
                it)
  captive-portal Captive portal commands
  crypto        Encryption related commands
  debug         Debugging functions
  logging       Modify message logging facilities
  page         Toggle paging
  service       Service Commands
  terminal      Set terminal line parameters
  upgrade       Remove a patch
  wireless      Wireless Configuration/Statistics commands
RFController#no
```

```
RFController(config)#no ?
  aaa-policy      Delete a aaa policy
  adoption-policy Delete an adoption policy
  advanced-wips-policy Delete an advanced-wips policy
  br650           Delete a Mobility 650 Access Point
  br7131          Delete a Mobility 7131 Series Access Point
  association-acl-policy Delete an association-acl policy
  captive-portal  Delete a captive portal
  critical-resource-policy Remove device onboard critical resource policy
  device-categorization Delete device categorization object
  dhcp-server-policy DHCP server policy
  dns-whitelist  Delete a whitelist object
  firewall-policy Configure firewall policy
  igmp-snoop-policy Remove device onboard igmp snoop policy
  ip             Internet Protocol (IP)
  mac            MAC configuration
  management-policy Delete a management policy
  nac-list        Delete an network access control list
```

## 6 Common Commands

|                                |                                                                                                          |
|--------------------------------|----------------------------------------------------------------------------------------------------------|
| password-encryption<br>profile | Disable password encryption in configuration<br>Delete a profile and all its associated<br>configuration |
| radio-qos-policy               | Delete a radio QoS configuration policy                                                                  |
| radius-group                   | Local radius server group configuration                                                                  |
| radius-server-policy           | Remove device onboard radius policy                                                                      |
| radius-user-pool-policy        | Configure Radius User Pool                                                                               |
| rf-domain                      | Delete a RF Domain and all its associated<br>configuration                                               |
| rfs4000                        | Delete a Mobility RFS4000 wireless controller                                                            |
| rfs6000                        | Delete a Mobility RFS6000 wireless controller                                                            |
| rfs7000                        | Delete a Mobility RFS7000 wireless controller                                                            |
| role-policy                    | Role based firewall policy                                                                               |
| smart-rf-policy                | Delete a smart-rf-policy                                                                                 |
| wips-policy                    | Delete a wips policy                                                                                     |
| wlan                           | Delete a wlan object                                                                                     |
| wlan-qos-policy                | Delete a wireless lan QoS configuration policy                                                           |
| service                        | Service Commands                                                                                         |
| aaa-policy                     | Delete a aaa policy                                                                                      |
| adoption-policy                | Delete an adoption policy                                                                                |
| advanced-wips-policy           | Delete an advanced-wips policy                                                                           |
| br650                          | Delete a Mobility 650 Access Point                                                                       |
| br6511                         | Delete a Mobility 6511 Access Point                                                                      |
| br6532                         | Delete a Mobility 6532 Access Point                                                                      |
| br7131                         | Delete a Mobility 7131 Series Access Point                                                               |
| association-acl-policy         | Delete an association-acl policy                                                                         |
| captive-portal                 | Delete a captive portal                                                                                  |
| critical-resource-policy       | Remove device onboard critical resource policy                                                           |
| customize                      | Restore the custom cli commands to default                                                               |
| device                         | Delete multiple devices                                                                                  |
| device-categorization          | Delete device categorization object                                                                      |
| dhcp-server-policy             | DHCP server policy                                                                                       |
| dns-whitelist                  | Delete a whitelist object                                                                                |
| event-system-policy            | Delete a event system policy                                                                             |
| firewall-policy                | Configure firewall policy                                                                                |
| igmp-snoop-policy              | Remove device onboard igmp snoop policy                                                                  |
| ip                             | Internet Protocol (IP)                                                                                   |
| mac                            | MAC configuration                                                                                        |
| management-policy              | Delete a management policy                                                                               |
| nac-list                       | Delete a network access control list                                                                     |
| password-encryption<br>profile | Disable password encryption in configuration<br>Delete a profile and all its associated<br>configuration |
| radio-qos-policy               | Delete a radio QoS configuration policy                                                                  |
| radius-group                   | Local radius server group configuration                                                                  |
| radius-server-policy           | Remove device onboard radius policy                                                                      |
| radius-user-pool-policy        | Configure Radius User Pool                                                                               |
| rf-domain                      | Delete one or more RF-domains and all their<br>associated configurations                                 |
| rfs4000                        | Delete a Mobility RFS4000 wireless controller                                                            |
| rfs6000                        | Delete a Mobility RFS6000 wireless controller                                                            |
| rfs7000                        | Delete a Mobility RFS7000 wireless controller                                                            |
| role-policy                    | Role based firewall policy                                                                               |
| smart-rf-policy                | Delete a smart-rf-policy                                                                                 |
| wips-policy                    | Delete a wips policy                                                                                     |
| wlan                           | Delete a wlan object                                                                                     |
| wlan-qos-policy                | Delete a wireless lan QoS configuration policy                                                           |
| service                        | Service Commands                                                                                         |

RFController(config)#



## show

### Common Commands

Displays running system information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show <parameter>
```

### Parameters

None

### Example

```
RFController>show ?
  adoption          Display information related to adoption to wireless
                    controller
  advanced-wips     Advanced WIPS
  captive-portal    Captive portal commands
  cdp               Cisco Discovery Protocol
  clock             Display system clock
  cluster           Cluster Protocol
  commands          Show command lists
  context           Information about current context
  critical-resources Critical Resources
  crypto            Encryption related commands
  debug             Debugging functions
  debugging         Debugging functions
  device-categorization Device Categorization
  event-history     Display event history
  firewall          Wireless Firewall
  interface         Interface Configuration/Statistics commands
  ip                Internet Protocol (IP)
  licenses          Show installed licenses and usage
  mac-address-table Display MAC address table
  mint              MiNT protocol
  noc               Noc-level information
  ntp               Network time protocol
  password-encryption Password encryption
  power            Show power over ethernet command
  remote-debug      Show details of remote debug sessions
  rf-domain-manager Show RF Domain Manager selection details
  role              Role based firewall
  running-config    Current operating configuration
  session-changes   Configuration changes made in this session
  session-config    This session configuration
```

## 6 Common Commands

|                             |                                           |
|-----------------------------|-------------------------------------------|
| <code>sessions</code>       | Display CLI sessions                      |
| <code>smart-rf</code>       | Smart-RF Management Commands              |
| <code>spanning-tree</code>  | Display spanning tree information         |
| <code>startup-config</code> | Startup configuration                     |
| <code>terminal</code>       | Display terminal configuration parameters |
| <code>timezone</code>       | The timezone                              |
| <code>version</code>        | Display software & hardware version       |
| <code>wireless</code>       | Wireless commands                         |

RFController>

## revert

### *Common Commands*

Reverts any changes made to their last saved configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
revert
```

### **Parameters**

None

### **Example**

```
RFController>revert  
RFController>
```

## service

### Common Commands

Service commands are used to manage the Controller configuration in all modes. Depending on the mode, different service commands display

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax User Exec Mode

```

service [advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster
|locator|noc|pktpcap|radio|set|show|smart-rf|wireless]

service advanced-wips [clear-event-history|terminate-device]
service advanced-wips clear-event-history [{accidental-association/all/
crackable-wep-iv-used/dos-cts-flood/dos-deauthentication-detection/
dos-disassociation-detection/dos-eap-failure-spoof/
dos-eapol-logoff-storm/dos-rts-flood/ssid-jack-attack-detected/
fake-dhcp-server-detected/fata-jack-detected/
id-theft-eapol-success-spoof-detected/
id-theft-out-of-sequence/invalid-channel-advertized/
invalid-management-frame/ipx-detection/
monkey-jack-attack-detected/multicast-all-routers-on-subnet/
multicast-all-systems-on-subnet/
multicast-dhcp-server-relay-agent/
multicast-hsrp-agent/multicast-igmp-detection/
multicast-igrmp-routers-detection/
multicast-ospf-all-routers-detection/
multicast-ospf-designated-routers-detection/
multicast-rip2-routers-detection/
multicast-vrrp-agent/netbios-detection/
null-probe-response-detected/probe-response-flood/rogue-ap-detection/
stp-detection/unathorized-bridge/windows-zero-config-memory-leak/
wlan-jack-attack-detected}]
service advanced-wips terminate-device <MAC>
service clear [ap-upgrade
history|command-history|noc|reboot-history|unsanctioned|upgrade-history|wirel
ess]
service clear [command-history|crash-info|reboot-history|
upgrade-history]{on <DEVICE-NAME>}
service clear noc statistics
service clear unsanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}}
service clear wireless [ap|client|radio|wlan]
service clear wireless ap statistics {<MAC>/on}
service clear wireless ap statistics <MAC> {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless ap statistics {on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless client statistics {<MAC>/on}
service clear wireless client statistics <MAC> {on <DEVICE-OR-DOMAIN-NAME>}

```

```

service clear wireless client statistics {on <DEVICE-OR-DOMAIN-NAME>}

service clear wireless radio statistics {<DEVICE-NAME>/on
<DEVICE-OR-DOMAIN-NAME>}
service clear wireless radio statistics <DEVICE-NAME> {<1-3>/on}
service clear wireless radio statistics <DEVICE-NAME> <1-3> {on
<DEVICE-OR-DOMAIN-NAME>}
service clear wireless radio statistics <DEVICE-NAME> {on
<DEVICE-OR-DOMAIN-NAME>}

service clear wireless wlan statistics {<WLAN>/on <DEVICE-OR-DOMAIN-NAME>}
service clear wireless wlan statistics <WLAN> {on <DEVICE-OR-DOMAIN-NAME>}

service cli-tables-expand {left/right}
service cli-tables-skin [ansi|hashes|minimal|none|percent|
stars|thick|thin|uf-8] {grid}
service cluster manual-revert
service locator {on <DEVICE-NAME>}
service noc parallel-updates <1-1024>

service pktcap on [bridge|deny|drop|ext-vlan|interface|radio|rim|router|
vpn|wireless] {acl-name <WORD>/count <1-1000000>/
direction[any|inbound|outbound]/filter <LINE>/hex/rate <1-100>/snap
<1-2048>/tcpdump/verbose/write [file/url/tzsp]}
service pktcap on interface [<WORD>/ge <1-4>/me1/port-channel <1-2>/vlan
<1-4094>]
service pktcap on radio [<1-3>|all]{acl-name <WORD>/count <1-1000000>
/direction [any|inbound|outbound]/filter <LINE>/hex/promiscuous/rate
<1-100>/snap <1-2048>/tcpdump/verbose/write [file/url/tzsp]}

service radio <1-3> [data-rates|dfs]
service radio <1-3> data-rates rate-index <0-27> [basic|supp]
service radio <1-3> dfs simulate-radar [extension|primary]

service set validation-mode [full|partial]{on <DEVICE-NAME>}

service show [advanced-wips|ap|captive-portal|cli|command-history|
crash-info|dhcp-lease|diag|info|mac-vendor <WORD>|mem|noc diag|pm|process|
reboot-history|rf-domain-manager|snmp session|startup-log|sys-info||top|
upgrade-history|watchdog|wireless|xpath-history]
service show advanced-wips stats
[ap-table|client-table|connected-sensors-status|termination-entries]
service show ap configured
service show captive-portal [servers|user-cache] {on <DEVICE-NAME>}
service show
[command-history|crash-info|info|mem|startup-log|process|sysinfo|top|upgrade-
history|watchdog] {on <DEVICE-NAME>}
service show dhcp-lease {<WORD>/on/vlan}
service show dhcp-lease <WORD> {on <DEVICE-NAME>}
service show dhcp-lease {on <DEVICE-NAME>}
service show dhcp-lease vlan <1-4094> {on <DEVICE-NAME>}
service show diag [led-status|stats] {on <DEVICE-NAME>}
service show pm {history/on <DEVICE-NAME>}
service show pm history {on <DEVICE-NAME>}
service show rf-domain-manager diag {<DEVICE-NAME/on>}
service show rf-domain-manager diag <DEVICE-NAME> {on <DEVICE-OR-DOMAIN-NAME>}
service show rf-domain-manager diag {on <DEVICE-OR-DOMAIN-NAME>}
service show [command-history|info|reboot-history|startup-log|
sys-info|upgrade-history|watchdog|xpath-history] {on <DEVICE-NAME>}}]

```

```

service show wireless
[clientap|config-internal|credential-cache|neighbors|stats-client|vlan-usage]
service show wireless ap diag {on <DEVICE-NAME>}
service show wireless client proc [info|stats]
service show wireless client proc [info|stats] {<MAC>/on}
service show wireless client proc [info|stats] <MAC> {on
<DEVICE-OR-DOMAIN-NAME>}
service show wireless client [info|stats] {on <DEVICE-OR-DOMAIN-NAME>}
service show wireless config-internal {include-factory}}]
service show wireless stats-client diag {<DEVICE-NAME>/on}
service show wireless stats-client diag <DEVICE-NAME> {on
<DEVICE-OR-DOMAIN-NAME>}
service show wireless stats-client diag {on <DEVICE-OR-DOMAIN-NAME>}
service show [crash-info|mem|process|top] {on <DEVICE-OR-DOMAIN-NAME>}
service smart-rf
[clear-config|clear-history|interactive-calibration|interactive-calibration-r
esult|run-calibration|stop-calibration]
service smart-rf
[clear-config|clear-history|interactive-calibration|run-calibration|stop-cali
bration]{on <DOMAIN-NAME>}
service smart-rf interactive-calibration-result
[discard|replace-current-config|write-to-configuration]{on <DOMAIN-NAME>}
service wireless [client|dump-core-snapshot|qos|wips]
service wireless client beacon-request <MAC> mode [active|passive|table]ssid
[<WORD>|any] channel-report [<WORD>|none]{on <DEVICE-NAME>}
service wireless qos delete-tspec <AA-BB-CC-DD-EE-FF> tid <0-7>
service wireless wips [clear-event-history|clear-muclient-blacklist]
service wireless wips clear-clientmu-blacklist [all|mac <AA-BB-CC-DD-EE-FF>
service wireless wips clear-event-history {on <DEVICE-OR-DOMAIN-NAME>}]

```

### Syntax Privilege Exec Mode

```

service
[advanced-wips|clear|cli-tables-expand|cli-tables-skin|cluster|copy|locator|m
int|noc|pktcap|pm|radio|set|show|signal|smart-rf|start-shell||wireless]
service copy tech-support [FILE|URL]
service clear
[ap-upgrade|command-history|crash-info|noc|reboot-history|unsanctioned|upgrad
e-history|wireless]
service mint [clear lsp-db|expire lsp|flood [csnp|lsp]|silence]
service signal [abort <WORD>|kill <WORD>]
service pm stop{on <DEVICE-NAME>}
service show [advanced-wips|captive-portal|cli|command-history|
crash-info|dhcp-lease|diag|info|last-passwd|mac-vendor|mem|noc|pm|process|reb
oot-history|rf-domain-manager|snmp|startup-log|sysinfo||top|upgrade-history|w
atchdog|wireless|
xpath-history]

```

### Syntax Global Config Mode

```

service [set|show cli]
service set [command-history <10-300>|upgrade-history <10-100>|
reboot-history <10-100>] {on <DEVICE-NAME>}

```

---

### NOTE

The parameters of the 'service' command of (User Exe, Privileged Exe, Global Config) are documented separately in 'Parameter Tables'.

---

## Parameters

advanced-wips [clear-event-history  
{accidental-association | |  
crackable-wep-iv-used | dos-cts-flood |  
dos-deauthentication-detection | dos-d  
isassociation-detection | dos-eap-failur  
e-spoof |  
dos-eapol-logoff-storm | dos-rts-flood |  
essid-jack-attack-detected |  
fake-dhcp-server-detected | fata-jack-d  
etected |  
id-theft-eapol-success-spoof-detected  
 |  
id-theft-out-of-sequence |  
invalid-channel-advertized | invalid-ma  
nagement-frame |  
ipx-detection | monkey-jack-attack-dete  
cted |  
multicast-all-routers-on-subnet |  
multicast-all-systems-on-subnet |  
multicast-dhcp-server-relay-agent | mul  
ticast-hsrp-agent | multicast-igmp-dete  
ction |  
multicast-igrp-routers-detection |  
multicast-ospf-all-routers-detection |  
multicast-ospf-designated-routers-det  
ection |  
multicast-rip2-routers-detection |

multicast-vrrp-agent | netbios-detectio  
n | null-probe-response-detected | prob  
e-response-flood | rogue-ap-detection |  
stp-detection

unauthorized-bridge | windows-zero-co  
nfig-memory-leak | wlan-jack-attack-de  
tected] | terminate-device <MAC>]

## Advanced-WIPS Commands

- clear-event-history – Clears the event history
  - accidental-association – Accidental client association
  - crackable-wep-iv-used – Crackable WEP IV Used
  - dos-cts-flood – DoS CTS flood
  - dos-deauthentication-detection – Detects DoS deauthentication
  - dos-disassociation-detection – Detects DoS disassociation
  - dos-eap-failure-spoof – Detects DoS EAP failure spoof
  - dos-eapol-logoff-storm – Detects DoS EAPoL logoff storm
  - dos-rts-flood – Detects DoS RTS flood
  - essid-jack-attack-detected – Detects ESSID jack attacks
  - fake-dhcp-server-detected – Detects fake DHCP server
  - fata-jack-detected – Detects fata-jack attacks
  - id-theft-eapol-success-spoof-detected – Detects IDs theft - EAPOL success spoof
  - id-theft-out-of-sequence – Detects IDs theft - out of sequence
  - invalid-channel-advertized – Detects invalid channel advertizement
  - invalid-management-frame – Detects invalid management frames
  - ipx-detection – Detects IPX
  - monkey-jack-attack-detected – Detects monkey-jack attacks
  - multicast-all-routers-on-subnet – Detects all multicast routers on the subnet
  - multicast-all-systems-on-subnet – Detects all multicast systems on the subnet
  - multicast-dhcp-server-relay-agent – Detects multicast DHCP server relay agents
  - multicast-hsrp-agent – Detects multicast HSRP agents
  - multicast-igmp-detection – Detects multicast IGMP
  - multicast-igrp-routers-detection – Detects multicast IGRP routers
  - multicast-ospf-all-routers-detection – Detects multicast OSPF all routers
  - multicast-ospf-designated-routers-detection – Detects multicast OSPF designated routers
  - multicast-rip2-routers-detection – Detects multicast RIP2 routers
  - multicast-vrrp-agent – Detects multicast VRRP agents
  - netbios-detection – Detects NetBIOS
  - null-probe-response-detected – Detects null probe response
  - probe-response-flood – Detects probe response flood
  - rogue-ap-detection – Detects rogue AP
  - stp-detection – Detects STP
- unauthorized-bridge – Unauthorized bridge detection
- windows-zero-config-memory-leak – Detects windows zero config memory leak
- wlan-jack-attack-detected – Detects WLAN jack attacks
- terminate-device <MAC> – Terminates an AP or client
  - <MAC> – MAC address of AP or client

## 6 Common Commands

---

|                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cli-tables-expand {left right}</code>                                                                                                    | Expands CLI table in dropdown format <ul style="list-style-type: none"><li>• left – Left justify output line</li><li>• right – Right justify output line</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>cli-tables-skin</code><br><code>[ansi hashes minimal none </code><br><code>percent stars thick </code><br><code>thin uf-8] {grid}</code> | Chooses a formatting layout/skin for CLI tabular outputs <ul style="list-style-type: none"><li>• ansi – Uses ANSI characters for borders</li><li>• hashes – Uses hashes (#) for borders</li><li>• minimal – Minimal, (one horizontal line between title and data rows)</li><li>• none – Space separated items, no decoration</li><li>• percent – Uses the percent sign (%) for borders</li><li>• stars – Use asterisks (*) for borders</li><li>• thick – Uses thick lines for borders</li><li>• thin – Uses thin lines for borders</li><li>• utf-8 – Uses UTF-8 characters for borders<ul style="list-style-type: none"><li>• grid – Optional. Uses a complete grid instead of title lines</li></ul></li></ul> |
| <code>cluster manual-revert</code>                                                                                                             | Cluster Protocol <ul style="list-style-type: none"><li>• manual-revert – Triggers manual revert on a standby controller</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>locator {on &lt;DEVICE-NAME&gt;}</code>                                                                                                  | Enables LEDs flashing on the device <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; – On AP/Controller<ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; – Displays AP/Controller information</li></ul></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>noc parallel-updates</code><br><code>&lt;1-1024&gt;</code>                                                                               | Configures NoC controller serviceability commands <ul style="list-style-type: none"><li>• parallel-updates &lt;1-1024&gt; – Sets the number of parallel threads limit from 1 to 1024</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |



```

pktpcap on [bridge|deny|
drop|ext-vlan|interface|
radio|rim|router|vpn|
|wireless]
{acl-name <WORD>|
count <1-1000000>
|direction|filter|hex|
rate <1-100>|snap
<1-2048>|
tcpdump|verbose|write
[file|url|tzsp]}

```

Starts the packet capture

- on – Enter the capture location from the list
  - bridge – Captures packets transiting through the ethernet bridge
  - deny – Captures packets denied by an ACL
  - drop – Captures packets at drop locations
  - ext-vlan – Captures packets forwarded to/from an extended VLAN
  - interface {<WORD>|ge <1-4>|me1|port-channel <1-2>|vlan <1-4094>} – Captures packets at a specified interface
    - <WORD> – Enter the interface name to capture packets
    - ge <1-4> – GigabitEthernet interface from 1-4
    - me1 – FastEthernet interface
    - port-channel <1-2> – Select a port-channel interface index from 1-2
    - vlan <1-4094> – Select a vlan id from 1-4094
  - radio [<1-3>|all] – Captures on a radio (802.11)
    - <1-3> – Select a radio index from 1-3
    - all – Selects all radios
  - rim – Captures packets at radio interface module
  - router – Captures packets transiting through IP router
  - vpn – Captures packets forwarded to/from a VPN link
  - wireless – Capture packets forwarded to/from wireless

The following parameters are common for the above:

- acl-name <WORD> – Specify the ACL that matches the acl-name for 'deny' location
- count <1-1000000> – Captures packet count from 1-1000000
- direction [any|inbound|outbound] – Changes the packet direction with respect to a device
  - any – Any direction
  - inbound – Inbound direction
  - outbound – Outbound direction
- filter <LINE> – Captures filter (must be last option)
  - <LINE> – Defines user defined packet capture filter
- hex – Provides binary output
- rate <1-100> – Specifies the rate at which the packets are captured per second
- snap <1-2048> – Captures the data length
- tcpdump – Decodes with TCP dump
- verbose – Provides verbose output

- write – Captures a file at a specified location
  - FILE Files: flash:/path/file  
cf:/path/file  
usb1:/path/file  
usb2:/path/file  
nvram:startup-config
    - URL – URLs: tftp://<hostname|IP>[:port]/path/file  
ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file  
sftp://<user>@<hostname|IP>[:port]/path/file
      - tzsp – Tazman Sniffer Protocol Host

## 6 Common Commands

---

|                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>radio &lt;1-3&gt; [data-rates rate-index &lt;0-27&gt; [basic supp]] dfs simulate-radar [extension primary]</code> | <p>Configures radio parameters</p> <ul style="list-style-type: none"><li>• &lt;1-3&gt; – Index value between 1 and 3</li><li>• data-rates rate-index &lt;0-27&gt; – Configures radio data rates<ul style="list-style-type: none"><li>• rate-index &lt;0-27&gt; [basic supp] – Specify a rate index between 0 and 27<ul style="list-style-type: none"><li>• basic – Specifies basic rates</li><li>• supp – Specifies supported rates</li></ul></li></ul></li><li>• dfs simulate-radar – Configures DFS related serviceability commands<ul style="list-style-type: none"><li>• simulate-radar [extension primary] – Simulates the presence of radar on a channel<ul style="list-style-type: none"><li>• extension – Simulates the presence of radar on the radios current extension channel</li><li>• primary – Simulates the presence of radar on the radios current primary channel</li></ul></li></ul></li></ul> |
| <code>set validation-mode [full partial] {on &lt;DEVICE-NAME&gt;}</code>                                                | <p>Sets validation mode</p> <ul style="list-style-type: none"><li>• validation-mode [full partial] – Displays the mode used to validate configuration settings<ul style="list-style-type: none"><li>• full {on &lt;DEVICE-NAME&gt;} – Uses full configuration validation</li><li>• partial {on &lt;DEVICE-NAME&gt;} – Uses partial configuration validation bypass<ul style="list-style-type: none"><li>• {on &lt;DEVICE-NAME&gt;} – On AP/Controller<ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; – Specifies the AP/Controller name</li></ul></li></ul></li></ul></li></ul>                                                                                                                                                                                                                                                                                                                       |

---

---

|                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>show [advanced-wips captive-portal cli command-history crash-info dhcp-lease diag info mac-vendor &lt;WORD&gt; mem noc pm process reboot-history rf-domain-manager diag {on &lt;DEVICE-NAME&gt;} snmp startup-log sysinfo  top upgrade-history watchdog wireless xpath-history]</pre> | <p>Displays the statistics about the running system</p> <ul style="list-style-type: none"> <li>• advanced-wips stats [ap-table client-table connected-sensors-status termination-entries] – Displays advanced-wips settings       <ul style="list-style-type: none"> <li>• stats – Displays advanced-wips statistics           <ul style="list-style-type: none"> <li>• ap-table – AP table</li> <li>• client-table – Client table</li> <li>• connected-sensors-status – Connected sensors</li> <li>• termination-entries – Termination entries</li> </ul> </li> </ul> </li> <li>• captive-portal[servers user-cache] – Displays captive portal commands       <ul style="list-style-type: none"> <li>• servers {on &lt;DEVICE-NAME&gt;} – Displays server information for active captive portals</li> <li>• user-cache {on &lt;DEVICE-NAME&gt;} – Displays cached user details for a captive portal</li> </ul> </li> <li>• command-history {on &lt;DEVICE-NAME&gt;} – Displays command history</li> <li>• crash-info {on &lt;DEVICE-NAME&gt;} – Displays information about core, panic and AP dump files</li> <li>• dhcp-lease {&lt;WORD&gt; on vlan} – Displays DHCP lease information received from the server       <ul style="list-style-type: none"> <li>• &lt;WORD&gt; on &lt;DEVICE-NAME&gt; – Specify the interface name</li> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• vlan &lt;1-4094&gt; on &lt;DEVICE-NAME&gt; – Specify a VLAN index between 1 and 4094           <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – AP/Controller name</li> </ul> </li> </ul> </li> <li>• diag [led-status stats] {on &lt;DEVICE-NAME&gt;} – Displays service show diag statistics commands       <ul style="list-style-type: none"> <li>• led-status – Displays LED's system status</li> <li>• stats – Displays system fan speed and sensor temperature</li> </ul> </li> <li>• info {on &lt;DEVICE-NAME&gt;} – Displays snapshot of available support information</li> <li>• mem {on &lt;DEVICE-NAME&gt;} – Displays the system's current memory usage</li> <li>• noc diag – Displays information regarding noc diagnostics</li> <li>• pm {history on &lt;DEVICE-NAME&gt;} – Displays information about process controlled by Process Monitor       <ul style="list-style-type: none"> <li>• history {on &lt;DEVICENAME&gt;} – Displays state changes for a process</li> </ul> </li> <li>• process {on &lt;DEVICENAME&gt;} – Displays active system process information</li> <li>• reboot-history {on &lt;DEVICE-NAME&gt;} – Displays the reboot history</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 
- rf-domain-manager diag {<DEVICE-NAME> | on} – Displays the RF Domain manager information
    - diag {<DEVICE-NAME> | on>} – Displays diagnostic information about RF Domain manager
      - <DEVICE-NAME> on <DEVICE-OR-DOMAIN-NAME> – Specify the MAC address of the device or its hostname
      - on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain
  - snmp session – Displays information regarding SNMP
    - session – Displays SNMP session information
  - startup-log {on <DEVICE-NAME>} – Displays the startup log
  - sysinfo {on <DEVICE-NAME>} – Displays the system's memory usage
  - upgrade-history {on <DEVICE-NAME>} – Displays the upgrade history of the specified device
  - xpath-history {on <DEVICE-NAME>} – Displays the xpath history of the specified device
  - top {on <DEVICE-OR-DOMAIN-NAME>} – Displays system resource information
  - watchdog {on <DEVICE-NAME>} – Displays watchdog status
  - wireless [client | config-internal | credential-cache | neighbors | stats-client | vlan-usage] – Displays wireless commands
    - client proc – Displays proc-entries for clients
      - proc [info | stats] – Dataplane proc entries
        - info {<MAC> | on} – Displays information about clients
        - stats {<MAC> | on} – Displays statistics about clients
        - <MAC> {on <DEVICE-OR-DOMAIN-NAME>} – Specify the MAC address of the client device
        - on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller
    - config-internal include-factory – Displays selected internal configuration parameters
      - include-factory – Includes factory default values
    - credential-cache – Displays the cached credentials (keys, vlan etc) of wireless clients
    - neighbors – Displays devices considered for neighbors, roaming and flow migration
    - stats-client diag – Displays information regarding managed Access Points
      - diag {<DEVICE-NAME> | on} – Displays diagnostic information about wireless AP
    - vlan-usage – Displays usage of VLANs across currently in-use wireless LANs
  - cli – Displays the CLI tree of current mode
  - mac-vendor <WORD> – Displays the vendor name for a given MAC address or OUI portion of a MAC address
- 
- noc diag – Displays information regarding noc updates
    - diag – Diagnostic information
  - pm [history | all] – Displays information about the processes controlled by process monitor
    - history – Displays the state changes for a process
    - on – On AP/Controller
      - <WORD> {on <DEVICE-NAME>} – Enter the process name
      - all {on <DEVICE-NAME>} – All processes

---

```
smart-rf [clear-config|
clear-history
|interactive-calibration
|run-calibration|
stop-calibration
|interactive-calibration-result]
```

#### Smart-RF Management Commands

- `clear-config {on <DOMAIN-NAME>}` – Clears the Smart RF configuration on all devices
- `clear-history {on <DOMAIN-NAME>}` – Clears the Smart RF history on all devices
- `interactive-calibration {on <DEVICE-NAME>}` – Interactive Smart RF calibration
- `run-calibration {on <DEVICE-NAME>}` – Starts a new calibration process
- `stop-calibration {on <DEVICE-NAME>}` – Stops the calibration currently in progress
- `interactive-calibration-result [discard|replace-current-config|write-to-configuration]` – Specifies interactive smart-rf calibration result
  - `discard {on <DOMAIN-NAME>}` – Discards interactive calibration results
  - `replace-current-config {on <DOMAIN-NAME>}` – Replaces current radio configuration
  - `write-to-configuration {on <DOMAIN-NAME>}` – Writes and saves radio settings to configuration

The following are the same for the above parameters:

- `on <DOMAIN-NAME>` – On RF-Domain
  - `<DOMAIN-NAME>` – RF-Domain name

clear [ap-upgrade|  
command-history|noc|  
reboot-history|  
upgrade-history|  
unsanctioned|wireless]

Performs a variety of reset functions

- command-history {on <DEVICE-NAME>} – Clears the command history
- reboot-history {on <DEVICE-NAME>} – Clears the reboot history
- upgrade-history {on <DEVICE-NAME>} – Clears the upgrade history

The following is common for the above:

- {on <DEVICE-NAME>} – On AP/Controller
  - <DEVICE-NAME> – AP/Controller name
- ap-upgrade history – Clears the AP upgrade history
- noc statistics – Clears noc related serviceability commands
  - statistics – Clears applicable statistics counters
- unsanctioned – Clears unsanctioned AP detection service commands
  - aps – Clears the list of all the unsanctioned APs detected
  - {on <DEVICE-OR-DOMAIN-NAME>} – On AP/Controller
    - <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF-Domain name
- wireless [ap|client|radio|wlan] – Clears the wireless commands
  - ap statistics – Clears wireless AP related serviceability commands
    - statistics {<MAC>|on} – Clears applicable AP statistics counters
  - client statistics – Clears wireless client related serviceability commands
    - statistics {<MAC>|on} – Clears applicable client statistics counters

The following are common for wireless ap and wireless client:

- { <MAC> on <DEVICE-OR-DOMAIN-NAME>} – Specify the MAC address of a particular wireless client
- {on <DEVICE-OR-DOMAIN-NAME>} – On AP/Controller/RF Domain
  - <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name
- radio statistics – Clears wireless radio related serviceability commands
  - statistics {<DEVICE-NAME>|on} – Clears applicable radio statistics counters
    - <DEVICE-NAME> {<1-3>|on} – Specify the hostname or MAC address
    - <1-3> {on <DEVICE-OR-DOMAIN-NAME>} – Specifies the radio interface index if not specified as part of radio ID
    - on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller/RF Domain name
- wlan statistics – Clears wireless WLAN related serviceability commands
  - statistics {<WLAN>|on} – Clears applicable WLAN statistics counters

- <WLAN> {on <DEVICE-OR-DOMAIN-NAME>} – Specify a WLAN name
- {on <DEVICE-OR-DOMAIN-NAME>} – On AP/Controller or RF Domain
  - <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF Domain name

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>wireless [client   dump-core-snapshot   qos   wips ]</pre> | <p>Configures wireless service commands</p> <ul style="list-style-type: none"> <li>client beacon-request &lt;MAC&gt; mode [active   passive   table] ssid [&lt;WORD&gt;   any] channel-report[&lt;WORD&gt;   none] {on &lt;DEVICE-NAME&gt;} – Configures wireless client service commands       <ul style="list-style-type: none"> <li>beacon-request &lt;MAC&gt; – Sends an 802.11k Beacon Measurement Request to a specified client           <ul style="list-style-type: none"> <li>&lt;MAC&gt; mode – Enter the MAC address of the client               <ul style="list-style-type: none"> <li>mode [active   passive   table] – Specify the mode in which the client must make the measurement                   <ul style="list-style-type: none"> <li>active – Requests the client to make the measurement in active mode</li> <li>passive – Requests the client to make the measurement in passive mode</li> <li>table – Requests the client to make the measurement in table mode</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>The following are common for the active, passive, and table sub-commands</p> <ul style="list-style-type: none"> <li>ssid[&lt;WORD&gt;   any] – Specify an SSID for which the measurements must be made       <ul style="list-style-type: none"> <li>[&lt;WORD&gt;   any] channel-report – Specify a particular SSID or any SSID           <ul style="list-style-type: none"> <li>channel-report[&lt;WORD&gt;   none] – Configures channel report in the request               <ul style="list-style-type: none"> <li>&lt;WORD&gt; {on &lt;DEVICE-NAME&gt;} – Specify a comma separated list of channels</li> <li>none {on &lt;DEVICE-NAME&gt;} – Applies to all channels</li> <li>on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>&lt;DEVICE-NAME&gt; – Specifies the AP/Controller name</li> </ul> </li> </ul> </li> <li>dump-core-snapshot – Triggers a debug core-dump of the wireless module</li> <li>qos – Wireless QoS related serviceability commands           <ul style="list-style-type: none"> <li>delete-tspec &lt;AA-BB-CC-DD-EE-FF&gt; – Sends a DELETE-TSPEC message to a specified client               <ul style="list-style-type: none"> <li>&lt;AA-BB-CC-DD-EE-FF&gt; rid – Enter the client MAC address</li> <li>tid &lt;0-7&gt; – Enter the traffic identifier from 0-7</li> </ul> </li> </ul> </li> </ul> </li> <li>wips [clear-event-history   clear-client-blacklist [all   mac &lt;AA-BB-CC-DD-EE-FF&gt;]] – Configures WIPS service commands       <ul style="list-style-type: none"> <li>clear-event-history {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Clears the event history           <ul style="list-style-type: none"> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller               <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – Specifies AP/Controller/RF Domain name</li> </ul> </li> </ul> </li> <li>clear-client-blacklist [all   mac &lt;AA-BB-CC-DD-EE-FF&gt;] – Clears the client information from blacklist           <ul style="list-style-type: none"> <li>all – Clears all clients from black-list</li> <li>mac &lt;AA-BB-CC-DD-EE-FF&gt; – Clears a specific client from the black-list               <ul style="list-style-type: none"> <li>&lt;AA-BB-CC-DD-EE-FF&gt; – Enter a client MAC address</li> </ul> </li> </ul> </li> </ul> </li> </ul> |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## ParametersPrivilege Exec Mode

|                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| copy tech-support [FILE URL]                                                                                                                                                                                                                           | <p>Copies files for technical support</p> <ul style="list-style-type: none"> <li>tech-support [&lt;file&gt; &lt;URL&gt;] [tftp ftp sftp] – Copies extensive system information useful to technical support for troubleshooting <ul style="list-style-type: none"> <li>FILE – File to which to copy <ul style="list-style-type: none"> <li>cf:/path/file</li> <li>usb1:/path/file</li> <li>usb2:/path/file</li> </ul> </li> <li>URL – Target URL from which to copy <ul style="list-style-type: none"> <li>tftp://&lt;hostname:port or IP&gt;/path/file</li> <li>ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;hostname:port or IP&gt;/path/file</li> <li>sftp://&lt;user&gt;@&lt;hostname:port or IP&gt;/path/file</li> </ul> </li> </ul> </li> </ul> |
| clear [ap-upgrade command-history crash-info noc reboot-history unsanctioned upgrade-history wireless]                                                                                                                                                 | <p>Same as 'User Exec' mode 'service clear' parameters except the crash-info parameter</p> <ul style="list-style-type: none"> <li>crash-info {on &lt;DEVICE-NAME&gt;} – Clears all crash files <ul style="list-style-type: none"> <li>{on &lt;DEVICE-NAME&gt;} – On AP/Controller</li> <li>&lt;DEVICE-NAME&gt; – AP/Controller name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| mint [clear lsp-db expire lsp flood[csnp lsp] silence]                                                                                                                                                                                                 | <p>Configures MiNT protocol parameters</p> <ul style="list-style-type: none"> <li>clear lsp-db – Resets functions <ul style="list-style-type: none"> <li>lsp-db – Clears the MiNT LSB database</li> </ul> </li> <li>expire lsp – Forces expiration <ul style="list-style-type: none"> <li>lsp – Forces expiration of the LSP</li> </ul> </li> <li>flood[csnp lsp] – Flood control packet <ul style="list-style-type: none"> <li>csnp – Floods our CSNP</li> <li>lsp – Flood our LSP</li> </ul> </li> <li>silence – Run silent</li> </ul>                                                                                                                                                                                                      |
| pm stop {on <DEVICE-NAME>}                                                                                                                                                                                                                             | <p>Process Monitor</p> <ul style="list-style-type: none"> <li>stop – Stops PM from monitoring all daemons <ul style="list-style-type: none"> <li>{on &lt;DEVICE-NAME&gt;} – On AP/Controller</li> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – AP/Controller/RF-Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| start-shell                                                                                                                                                                                                                                            | Provides shell access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| signal [abort <WORD> kill <WORD>]                                                                                                                                                                                                                      | <p>Sends a signal to a process</p> <ul style="list-style-type: none"> <li>abort &lt;WORD&gt; – Sends an abort signal (to force it to dump core)</li> <li>kill &lt;WORD&gt; – Sends a kill signal (terminate without a core)</li> <li>&lt;WORD&gt; – Enter the name of process to be signalled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| show [advanced-wips captive-portal cli command-history crash-info dhcp-lease diag info last-passwd mac-vendor <WORD> mem noc pm process reboot-history rf-domain-manager snmp startup-log sysinfo top upgrade-history watchdog wireless xpath-history] | <p>Same as 'User Exec' Mode 'service show' parameters except 'last-passwd' parameter</p> <ul style="list-style-type: none"> <li>last-passwd – Displays the last password used to enter the shell service</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



**ParametersGlobal Config Mode**


---

|                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set [command history<br><10-300> upgrade history<br><10-100> reboot history<br><10-100>] {on<br><DEVICE-NAME>} | Defines validation mode settings <ul style="list-style-type: none"> <li>• command history &lt;10-300&gt; – Sets the size of command history. The default size is 200)</li> <li>• reboot history &lt;10-100&gt; – Sets the size of the reboot history. The default size is 50.</li> <li>• upgrade history &lt;10-100&gt; – Sets the size of the upgrade history. The default size is 50.             <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – On AP/Controller                 <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – AP/Controller name</li> </ul> </li> </ul> </li> </ul> |
| show cli                                                                                                       | Displays running system configuration <ul style="list-style-type: none"> <li>• cli – Displays the CLI tree of the current mode</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

---

**Example**

```

RFController>service cli-tables-skin stars
RFController>

RFController>service pktcap on interface vlan 2
Capturing up to 50 packets. Use Ctrl-C to abort.

RFController>service show cli
User Exec mode: +-do
+-help [help]
  +-show
    +-configuration-tree [help show configuration-tree]
  +-search
    +-WORD [help search WORD (|detailed|only-show|skip-show)]
      +-detailed [help search WORD (|detailed|only-show|skip-show)]
      +-only-show [help search WORD (|detailed|only-show|skip-show)]
      +-skip-show [help search WORD (|detailed|only-show|skip-show)]
  +-show
    +-commands [show commands]
    +-running-config [show (running-config|session-config) (|include-factory)]
      +-include-factory [show (running-config|session-config)
(|include-factory)]
        +-interface [show running-config interface (|`WORD|ge <1-4>|me1|pc
<1-4>|vlan <1-4094>') (|include-factory)]
          +-WORD [show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>') (|include-factory)]
            +-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan <1-4094>') (|include-factory)]
              +-ge
                +-<1-4> [show running-config interface (|`WORD|ge <1-4>|me1|pc
<1-4>|vlan <1-4094>') (|include-factory)]
                  +-include-factory [show running-config interface (|`WORD|ge
<1-4>|me1|pc <1-4>|vlan <1-4094>')
(|include-factory)].....
.....RFController>

RFController>service show general stats on RFController
Current Fan Speed: 6540 Minimum Fan Speed: TBD Hysteresis: TBD

Sensor 1 Temperature: 31C
Sensor 2 Temperature: 55C
Sensor 3 Temperature: 29C
Sensor 4 Temperature: 28C
Sensor 5 Temperature: 26C

```

## 6 Common Commands

```
Sensor 6 Temperature: 28C
```

```
RFController>
```

```
RFController>service wireless wips clear-mu-blacklist mac 11-22-33-44-55-66  
RFController>
```

```
RFController#service signal kill testp  
Sending a kill signal to testp  
RFController#  
RFController#service signal abort testprocess  
Sending an abort signal to testprocess  
RFController#
```

```
RFController#service mint clear lsp-db  
RFController#
```

```
RFController#service mint silence  
RFController#
```

```
RFController#service pm stop on RFController  
RFController#
```

```
RFController(config)#service show cli  
Global Config mode:  
+-help [help]  
  +-search  
    +-WORD [help search WORD (|detailed|only-show|skip-show)]  
    +-detailed [help search WORD (|detailed|only-show|skip-show)]  
    +-only-show [help search WORD (|detailed|only-show|skip-show)]  
    +-skip-show [help search WORD (|detailed|only-show|skip-show)]  
+-show  
  +-commands [show commands]  
  +-eval  
    +-LINE [show eval LINE]  
  +-debugging [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]  
    +-cfgd [show debugging cfgd]  
    +-on  
      +-DEVICE-OR-DOMAIN-NAME [show debugging (|(on DEVICE-OR-DOMAIN-NAME))]  
    +-wireless [show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))]  
      +-on  
        +-DEVICE-OR-DOMAIN-NAME [show debugging wireless (|(on  
DEVICE-OR-DOMAIN-NAME))]  
      +-voice [show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))]  
        +-on  
          +-DEVICE-OR-DOMAIN-NAME [show debugging voice (|(on  
DEVICE-OR-DOMAIN-NAME))]  
      +-captive-portal [show debugging captive-portal (|(on  
DEVICE-OR-DOMAIN-NAME))]  
        +-on  
          +-DEVICE-OR-DOMAIN-NAME [show debugging captive-portal (|(on  
DEVICE-OR-DOMAIN-NAME))]  
      +-dhcpsvr [show debugging dhcpsvr (|(on DEVICE-NAME))]  
        +-on.....  
RFController(config)#
```

```
RFController#service traceroute -h  
traceroute: invalid option -- h  
BusyBox v1.14.1 () multi-call binary
```

```
Usage: traceroute [-Fildnr] [-f 1st_ttl] [-m max_ttl] [-p port#] [-q
nqueries]
      [-s src_addr] [-t tos] [-w wait] [-g gateway] [-i iface]
      [-z pausemsecs] HOST [data size]
```

Trace the route to HOST

Options:

```
-F      Set the don't fragment bit
-I      Use ICMP ECHO instead of UDP datagrams
-l      Display the ttl value of the returned packet
-d      Set SO_DEBUG options to socket
-n      Print hop addresses numerically rather than symbolically
-r      Bypass the normal routing tables and send directly to a host
-v      Verbose
-m max_ttl      Max time-to-live (max number of hops)
-p port#      Base UDP port number used in probes
              (default is 33434)
-q nqueries    Number of probes per 'ttl' (default 3)
-s src_addr    IP address to use as the source address
-t tos        Type-of-service in probe packets (default 0)
-w wait       Time in seconds to wait for a response
              (default 3 sec)
-g           Loose source route gateway (8 max)
```

RFController#

RFController>ser show ap configured

```
-----
IDX      NAME          MAC          PROFILE      RF-DOMAIN    ADOPTED-BY
-----
1   br7131-889EC4  00-15-70-88-9E-C4  default-br7131  default      un-adopted
2   br650-445566  11-22-33-44-55-66  default-br650   default      un-adopted
3   br650-000000  00-A0-F8-00-00-00  default-br650   default      00-15-70-37-FA-BE
-----
```

RFController>

RFController>service show command-history on RFController  
Configured size of command history is 200

```
Date & Time          User      Location          Command
=====
Jul 28 16:39:34 2010  admin    172.16.10.10 17 service locator on RFController
Jul 28 16:39:13 2010  admin    172.16.10.10 17      exit
Jul 28 16:17:51 2010  admin    172.16.10.10 17      exit
Jul 28 16:15:58 2010  admin    172.16.10.10 17      exit
Jul 28 16:15:53 2010  admin    172.16.10.10 17      advanced-wips-policy test
Jul 28 16:08:13 2010  admin    172.16.10.10 17      exit
Jul 28 15:24:25 2010  admin    172.16.10.10 16      firewall-policy test
Jul 28 13:51:59 2010  admin    172.16.10.10 15      exit
Jul 28 13:51:47 2010  admin    172.16.10.10 15      exit
Jul 28 13:51:44 2010  admin    172.16.10.10 15      exit
Jul 28 13:51:43 2010  admin    172.16.10.10 15      exit
Jul 28 13:21:17 2010  admin    172.16.10.10 15      aaa-policy test
Jul 28 13:20:35 2010  admin    172.16.10.10 15      exit
Jul 28 13:09:14 2010  admin    172.16.10.10 15      exit
Jul 28 13:08:44 2010  admin    172.16.10.10 15      aaa-policy test
Jul 27 13:46:46 2010  admin    172.16.10.10 6       ip nat pool pool1
prefix-length 1
```

## 6 Common Commands

```
Jul 27 13:44:46 2010 admin 172.16.10.10 6 profile rfs7000
default-rfs7000
Jul 27 12:39:29 2010 admin 172.16.10.12 5 reload force
Jul 27 12:28:41 2010 admin 172.16.10.12 20 reload force
Jul 27 12:28:39 2010 admin 172.16.10.12 20 write memory
.....
RFController>
```

```
RFController>service show diag stats on RFController
```

```
fan 1 current speed: 6660 min_speed: 2000 hysteresis: 250
fan 2 current speed: 6720 min_speed: 2000 hysteresis: 250
fan 3 current speed: 6540 min_speed: 2000 hysteresis: 250
```

```
Sensor 1 Temperature 32.0 C
Sensor 2 Temperature 58.0 C
Sensor 3 Temperature 29.0 C
Sensor 4 Temperature 28.0 C
Sensor 5 Temperature 26.0 C
Sensor 6 Temperature 28.0 C
```

```
RFController>service show info on RFController
7.7M out of 8.0M available for logs.
9.4M out of 10.0M available for history.
19.2M out of 20.0M available for crashinfo.
```

```
List of Files:
```

|                 |       |              |
|-----------------|-------|--------------|
| cfgd.log        | 5.7K  | Jul 28 17:17 |
| fmgr.log        | 221   | Jul 27 12:40 |
| messages.log    | 1.0K  | Jul 27 12:41 |
| startup.log     | 52.3K | Jul 27 12:40 |
| command.history | 903   | Jul 28 16:39 |
| reboot.history  | 1.6K  | Jul 27 12:40 |
| upgrade.history | 698   | Jul 27 12:39 |

```
Please export these files or delete them for more space.
```

```
RFController>
```

```
RFController>service show upgrade-history on RFController
Configured size of upgrade history is 50
```

| Date & Time                                                             | Old Version  | New Version  | Status                     |
|-------------------------------------------------------------------------|--------------|--------------|----------------------------|
| Jul 27 12:37:30 2010                                                    | 5.0.0.0-098D | 5.0.0.0-097B | Successful                 |
| Jul 27 12:26:34 2010                                                    | 5.0.0.0-097B | 5.0.0.0-098D | Successful                 |
| Jul 22 16:33:04 2010                                                    | 5.0.0.0-096B | 5.0.0.0-097B | Successful                 |
| Jul 22 16:32:15 2010                                                    | 5.0.0.0-096B | 5.0.0.0-096B | Unable to get update file. |
| ftpget: cannot connect to remote host (172.16.10.1): Connection refused |              |              |                            |
| Jul 19 17:51:29 2010                                                    | 5.0.0.0-090D | 5.0.0.0-096B | Successful                 |
| Jul 12 12:41:12 2010                                                    | 5.0.0.0-088D | 5.0.0.0-090D | Successful                 |
| Jul 06 12:38:49 2010                                                    | 5.0.0.0-086D | 5.0.0.0-088D | Successful                 |
| Jun 29 13:06:50 2010                                                    | 5.0.0.0-084D | 5.0.0.0-086D | Successful                 |

```
.....
RFController
```

```
RFController>service show watchdog
```

```
watchdog is enabled
countdown: 255 seconds of 260 remain until reset
RFController>
```

```
RFController>service show xpath-history
```

```
-----
DATE&TIME                USER                XPATH                DURATION(MS)
-----
Wed Jul 28 17:29:49 2010 [system]
/wing-stats/device/00-A0-F8-00-00-00/_internal/adjust_stats_interval 40
Wed Jul 28 17:29:49 2010 [system]
/wing-stats/device/00-15-70-37-FA-BE/_internal/adjust_stats_interval 16
Wed Jul 28 17:29:43 2010 [system]
/wing-stats/device/00-A0-F8-00-00-00/_internal/adjust_stats_interval 39
Wed Jul 28 17:29:43 2010 [system]
/wing-stats/device/00-15-70-37-FA-BE/_internal/adjust_stats_interval 16
Wed Jul 28 17:29:37 2010 [system]
/wing-stats/device/00-A0-F8-00-00-00/_internal/adjust_stats_interval 40
Wed Jul 28 17:29:37 2010 [system]
/wing-stats/device/00-15-70-37-FA-BE/_internal/adjust_stats_interval 17
Wed Jul 28 17:29:31 2010 [system]
/wing-stats/device/00-A0-F8-00-00-00/_internal/adjust_stats_interval 40
Wed Jul 28 17:29:31 2010 [system]
/wing-stats/device/00-15-70-37-FA-BE/_internal/adjust_stats_interval 16
Wed Jul 28 17:29:30 2010 [system]
/wing-stats/device/00-15-70-37-FA-BE/watchdog-status 6
-----
```

```
RFController#service show last-passwd
```

```
Last password used: password with MAC 00:15:70:37:fa:be
RFController#
```

```
RFController>service show wireless ap diag on RFController
```

```
-----
AP-MAC                    FIELD                VALUE
-----
00-15-70-37-FA-BE        is_manager           True
00-15-70-37-FA-BE        last_stats_upload    107802.617188
00-15-70-37-FA-BE        manager_mint_id      70.37.FA.BE
00-15-70-37-FA-BE        max_pull_time        2.80668640137
00-15-70-37-FA-BE        num_adoptions        0
00-15-70-37-FA-BE        num_config_applied   0
00-15-70-37-FA-BE        num_config_failed    0
00-15-70-37-FA-BE        num_config_received  0
00-15-70-37-FA-BE        num_stats_pulled     17951
00-15-70-37-FA-BE        num_stats_pushed     0
00-15-70-37-FA-BE        upload_state         master
-----
AP-MAC                    FIELD                VALUE
-----
00-A0-F8-00-00-00        is_manager           False
00-A0-F8-00-00-00        last_stats_upload    449767.65625
00-A0-F8-00-00-00        manager_mint_id      70.37.FA.BE
00-A0-F8-00-00-00        max_pull_time        0
00-A0-F8-00-00-00        num_adoptions        2
00-A0-F8-00-00-00        num_config_applied   2
00-A0-F8-00-00-00        num_config_failed    0
00-A0-F8-00-00-00        num_config_received  2
00-A0-F8-00-00-00        num_stats_pulled     74796
00-A0-F8-00-00-00        num_stats_pushed     3
00-A0-F8-00-00-00        upload_state         connected
-----
```

```
Total number of APs displayed: 2
```

```
RFController>
```

## 6 Common Commands

```
RFController>service show wireless config-internal
! Startup-Config-Playback Completed: Yes
no debug wireless
no country-code
!
wlan-qos-policy default
no rate-limit wlan to-air
no rate-limit wlan from-air
no rate-limit client to-air
no rate-limit client from-air
!
wlan wlan1
ssid wlan1
vlan 1
qos-policy default
encryption-type none
authentication-type none
no accounting radius
no accounting syslog
RFController>
```

### System Information:

```
Free RAM: 68.0% (169 of 249) Min: 10.0%
File Descriptors: free: 24198 used: 960 max: 25500
CPU load averages: 1 min: 0.0% 5 min: 0.0% 15 min: 0.0%
```

### Kernel Buffers:

|        |       |      |      |      |      |      |       |       |      |     |     |     |
|--------|-------|------|------|------|------|------|-------|-------|------|-----|-----|-----|
| Size:  | 32    | 64   | 128  | 256  | 512  | 1k   | 2k    | 4k    | 8k   | 16k | 32k | 64k |
| Usage: | 2761  | 2965 | 927  | 201  | 549  | 107  | 141   | 25    | 68   | 0   | 1   | 2   |
| Limit: | 32768 | 8192 | 4096 | 4096 | 8192 | 8192 | 16384 | 16384 | 1024 | 512 | 256 | 64  |

```
RFController#
```

```
RFController>service clear wireless radio statistics on RFController
clear radio stats on *: o.k.
```

```
RFController#service show dhcp-lease vlan 1 on RFController
No dhcp lease information available
RFController#
```

## write

### Common Commands

Writes the system running configuration to memory or terminal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
write
```

### Parameters

|          |                     |
|----------|---------------------|
| memory   | Writes to NV memory |
| terminal | Writes to terminal  |

### Example

```
RFController>write memory
[OK]
RFController>
```

```
RFController>write terminal
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
enable
calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
voice-prioritization
svp-prioritization
wmm background cw-max 8
wmm video txop-limit 9
.....
RFController>
```

## 6 Common Commands



# Show Commands

---

## In this chapter

- [show commands](#) ..... 319

This chapter provides an overview of all the show commands within the controller CLI structure.

This chapter describes the 'show' CLI commands used in the USER EXEC, PRIV EXEC, and GLOBAL CONFIG modes. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If a user or privilege is not specified, the referenced command can be entered in either mode.

This chapter describes the 'show' commands in the 'GLOBAL CONFIG' mode. All the commands in this chapter can be entered in all the three modes except commands like file, ip-access-list-stats, mac-access-list-stats and upgrade stats commands, which cannot be entered in the User Executable Mode.

## show commands

[Table 15](#) Summarizes show commands

**TABLE 15** show Commands

| Command                            | Description                                              | Reference                |
|------------------------------------|----------------------------------------------------------|--------------------------|
| <a href="#">show</a>               | Displays the settings for the specified system component | <a href="#">page 322</a> |
| <a href="#">adoption</a>           | Displays information related to controller adoption      | <a href="#">page 326</a> |
| <a href="#">advanced-wips</a>      | Displays advanced-wips settings                          | <a href="#">page 328</a> |
| <a href="#">ap-upgrade</a>         | Displays Access Point software image upgrade information | <a href="#">page 331</a> |
| <a href="#">boot</a>               | Displays a device boot configuration                     | <a href="#">page 332</a> |
| <a href="#">captive-portal</a>     | Displays WLAN hotspot functions                          | <a href="#">page 333</a> |
| <a href="#">cdp</a>                | Displays a Cisco Discovery Protocol neighbor table       | <a href="#">page 335</a> |
| <a href="#">clock</a>              | Displays the software system clock                       | <a href="#">page 336</a> |
| <a href="#">cluster</a>            | Displays cluster commands                                | <a href="#">page 337</a> |
| <a href="#">commands</a>           | Displays command list                                    | <a href="#">page 338</a> |
| <a href="#">context</a>            | Displays information about the current context           | <a href="#">page 340</a> |
| <a href="#">critical-resources</a> | Displays critical-resource information                   | <a href="#">page 342</a> |
| <a href="#">crypto</a>             | Displays encryption mode information                     | <a href="#">page 343</a> |
| <a href="#">debug</a>              | Displays debugging configuration information             | <a href="#">page 346</a> |
| <a href="#">debugging</a>          | Displays debugging configuration information             | <a href="#">page 348</a> |

**TABLE 15** show Commands

| <b>Command</b>               | <b>Description</b>                                                  | <b>Reference</b>         |
|------------------------------|---------------------------------------------------------------------|--------------------------|
| <i>device-categorization</i> | Displays device categorization details                              | <a href="#">page 348</a> |
| <i>event-history</i>         | Displays the event history                                          | <a href="#">page 351</a> |
| <i>event-system-policy</i>   | Displays event system policy configuration information in detail    | <a href="#">page 352</a> |
| <i>file</i>                  | Displays file system information                                    | <a href="#">page 353</a> |
| <i>firewall</i>              | Displays wireless firewall information                              | <a href="#">page 354</a> |
| <i>interface</i>             | Displays the status of the different controller interfaces          | <a href="#">page 358</a> |
| <i>ip</i>                    | Displays Internet Protocol (IP) related information                 | <a href="#">page 360</a> |
| <i>ip-access-list-stats</i>  | Displays IP access list stats                                       | <a href="#">page 364</a> |
| <i>licenses</i>              | Displays installed licenses and usage information                   | <a href="#">page 365</a> |
| <i>lldp</i>                  | Displays Link Layer Discovery Protocol information on AP/Controller | <a href="#">page 366</a> |
| <i>lldp</i>                  | Displays logging information                                        | <a href="#">page 366</a> |
| <i>mac-access-list-stats</i> | Displays MAC access list statistics                                 | <a href="#">page 369</a> |
| <i>mac-address-table</i>     | Displays MAC address table entries                                  | <a href="#">page 370</a> |
| <i>mint</i>                  | Displays MINT protocol configuration commands                       | <a href="#">page 371</a> |
| <i>noc</i>                   | Displays Noc-level information                                      | <a href="#">page 373</a> |
| <i>ntp</i>                   | Displays <i>Network Time Protocol</i> (NTP) information             | <a href="#">page 376</a> |
| <i>password-encryption</i>   | Displays password encryption status information                     | <a href="#">page 377</a> |
| <i>power</i>                 | Displays power over ethernet (PoE) information                      | <a href="#">page 378</a> |
| <i>remote-debug</i>          | Displays remote debug session data                                  | <a href="#">page 380</a> |
| <i>rf-domain-manager</i>     | Displays RF Domain manager selection details                        | <a href="#">page 381</a> |
| <i>role</i>                  | Displays role based firewall information                            | <a href="#">page 382</a> |
| <i>running-config</i>        | Displays the contents of configuration files                        | <a href="#">page 383</a> |
| <i>session-changes</i>       | Displays the configuration changes made in this session             | <a href="#">page 385</a> |
| <i>session-config</i>        | Displays the list of currently active open sessions on the device   | <a href="#">page 386</a> |
| <i>sessions</i>              | Displays CLI sessions                                               | <a href="#">page 387</a> |
| <i>smart-rf</i>              | Displays Smart RF Management commands                               | <a href="#">page 388</a> |
| <i>spanning-tree</i>         | Displays spanning-tree information                                  | <a href="#">page 390</a> |
| <i>startup-config</i>        | Displays the complete startup configuration script on the console   | <a href="#">page 393</a> |
| <i>terminal</i>              | Displays terminal configuration parameters                          | <a href="#">page 394</a> |
| <i>timezone</i>              | Displays the status of the image upgrade                            | <a href="#">page 395</a> |
| <i>upgrade-status</i>        | Displays the upgrade status                                         | <a href="#">page 396</a> |

**TABLE 15** show Commands

| <b>Command</b>           | <b>Description</b>                                       | <b>Reference</b>         |
|--------------------------|----------------------------------------------------------|--------------------------|
| <a href="#">version</a>  | Displays the software and hardware version on the device | <a href="#">page 397</a> |
| <a href="#">wireless</a> | Displays wireless configuration parameters               | <a href="#">page 398</a> |
| <a href="#">wwan</a>     | Displays wireless WAN status                             | <a href="#">page 405</a> |

## show

### *show commands*

Displays the settings for the specified system component. There are a number of ways to invoke the show command:

- When invoked without any arguments, it displays information about the current context. If the current context contains instances, the show command (usually) displays a list of these instances.
- When invoked with the display parameter, it displays information about that component.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
show <parameter>
```

### **Parameters**

None

### **Example**

### *Global Config Mode*

|                       |                                                                |
|-----------------------|----------------------------------------------------------------|
| adoption              | Display information related to adoption to wireless controller |
| advanced-wips         | Advanced WIPS                                                  |
| ap-upgrade            | AP Upgrade                                                     |
| boot                  | Display boot configuration.                                    |
| captive-portal        | Captive portal commands                                        |
| cdp                   | Cisco Discovery Protocol                                       |
| clock                 | Display system clock                                           |
| cluster               | Cluster Protocol                                               |
| commands              | Show command lists                                             |
| context               | Information about current context                              |
| critical-resources    | Critical Resources                                             |
| crypto                | Encryption related commands                                    |
| debug                 | Debugging functions                                            |
| debugging             | Debugging functions                                            |
| device-categorization | Device Categorization                                          |
| event-history         | Display event history                                          |
| event-system-policy   | Display event system policy                                    |
| file                  | Display filesystem information                                 |
| firewall              | Wireless Firewall                                              |
| interface             | Interface Configuration/Statistics commands                    |
| ip                    | Internet Protocol (IP)                                         |

|                       |                                            |
|-----------------------|--------------------------------------------|
| ip-access-list-stats  | IP Access list stats                       |
| licenses              | Show installed licenses and usage          |
| lldp                  | Link Layer Discovery Protocol              |
| logging               | Show logging information                   |
| mac-access-list-stats | MAC Access list stats                      |
| mac-address-table     | Display MAC address table                  |
| mint                  | MiNT protocol                              |
| noc                   | Noc-level information                      |
| ntp                   | Network time protocol                      |
| password-encryption   | Pasword encryption                         |
| power                 | Show power over ethernet command           |
| remote-debug          | Show details of remote debug sessions      |
| rf-domain-manager     | Show RF Domain Manager selection details   |
| role                  | Role based firewall                        |
| running-config        | Current operating configuration            |
| session-changes       | Configuration changes made in this session |
| session-config        | This session configuration                 |
| sessions              | Display CLI sessions                       |
| smart-rf              | Smart-RF Management Commands               |
| spanning-tree         | Display spanning tree information          |
| startup-config        | Startup configuration                      |
| terminal              | Display terminal configuration parameters  |
| timezone              | The timezone                               |
| upgrade-status        | Display last image upgrade status          |
| version               | Display software & hardware version        |
| wireless              | Wireless commands                          |
| wwan                  | Display wireless WAN Status                |

```
RFController(config)# show clock on RFController
Apr 08 14:21:40 UTC 2010
RFController(config)#
```

## ***PRIVILEGE EXEC Mode***

```
RFController#show ?
RFController#show ?
adoption                Display information related to adoption to wireless
                        controller
advanced-wips           Advanced WIPS
ap-upgrade              AP Upgrade
boot                    Display boot configuration.
captive-portal          Captive portal commands
cdp                     Cisco Discovery Protocol
clock                   Display system clock
cluster                 Cluster Protocol
commands                Show command lists
context                 Information about current context
critical-resources      Critical Resources
crypto                  Encryption related commands
debug                   Debugging functions
debugging               Debugging functions
device-categorization  Device Categorization
event-history           Display event history
event-system-policy     Display event system policy
file                    Display filesystem information
firewall                Wireless Firewall
interface               Interface Configuration/Statistics commands
ip                       Internet Protocol (IP)
```

## 7 show commands

```
ip-access-list-stats    IP Access list stats
licenses                Show installed licenses and usage
lldp                    Link Layer Discovery Protocol
logging                 Show logging information
mac-access-list-stats  MAC Access list stats
mac-address-table      Display MAC address table
mint                    MiNT protocol
noc                     Noc-level information
ntp                     Network time protocol
password-encryption    Pasword encryption
power                   Show power over ethernet command
remote-debug            Show details of remote debug sessio
rf-domain-manager      Show RF Domain Manager selection de
role                    Role based firewall
running-config          Current operating configuration
session-changes         Configuration changes made in this
session-config          This session configuration
sessions                Display CLI sessions
smart-rf                Smart-RF Management Commands
spanning-tree           Display spanning tree information
startup-config          Startup configuration
terminal                Display terminal configuration para
timezone                The timezone
upgrade-status          Display last image upgrade status
version                 Display software & hardware version
wireless                Wireless commands
wwan                    Display wireless WAN Status
```

```
RFController#
```

```
RFController#show terminal
Terminal Type: xterm
Length: 45      Width: 126
RFController#
```

### ***USER EXEC Mode***

```
RFController>show ?
adoption                Display information related to adoption to wireless
                        controller
advanced-wips           Advanced WIPS
ap-upgrade              AP Upgrade
captive-portal          Captive portal commands
cdp                     Cisco Discovery Protocol
clock                   Display system clock
cluster                 Cluster Protocol
commands                Show command lists
context                 Information about current context
critical-resources      Critical Resources
crypto                  Encryption related commands
debug                   Debugging functions
debugging               Debugging functions
device-categorization  Device Categorization
event-history            Display event history
event-system-policy     Display event system policy
firewall                Wireless Firewall
interface                Interface Configuration/Statistics commands
ip                       Internet Protocol (IP)
```

```

licenses          Show installed licenses and usage
lldp              Link Layer Discovery Protocol
logging          Show logging information
mac-address-table Display MAC address table
mint             MiNT protocol
noc              Noc-level information
ntp              Network time protocol
password-encryption Password encryption
power            Show power over ethernet command
remote-debug     Show details of remote debug sessions
rf-domain-manager Show RF Domain Manager selection details
role            Role based firewall
running-config   Current operating configuration
session-changes  Configuration changes made in this session
session-config   This session configuration
sessions         Display CLI sessions
smart-rf         Smart-RF Management Commands
spanning-tree    Display spanning tree information
startup-config   Startup configuration
terminal         Display terminal configuration parameters
timezone        The timezone
version          Display software & hardware version
wireless         Wireless commands
wwan             Display wireless WAN Status

```

```
RFController>
```

```
RFController>show wireless ap configured
```

```

-----
IDX      NAME                MAC                PROFILE            RF-DOMAIN          ADOPTED-BY
-----
1    br7131-889EC4    00-15-70-88-9E-C4    default-br7131    default            un-adopted
2    br650-445566    11-22-33-44-55-66    default-br650    default            un-adopted
-----

```

```
RFController>
```

## adoption

### show commands

Displays information related to controller adoption

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show adoption [config-errors <DEVICE-NAME>|history {on <DEVICE-NAME>}
|info|offline|pending]
```

### Parameters

---

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| adoption [info offline] | <p>Displays the current adoption status of an access point</p> <ul style="list-style-type: none"> <li>• config-errors &lt;DEVICE-NAME&gt; – Displays the configuration errors of adopted access points <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller</li> </ul> </li> <li>• info – Displays the adoption status of the device and its adopted access points</li> <li>• offline – Displays the unadopted status of the device and its adopted access points</li> <li>• history {on &lt;DEVICE-NAME&gt;} – Displays the adoption history status of the device and its adopted access points</li> <li>• pending {on &lt;DEVICE-NAME&gt;} – Displays the information related to non adopted access points <ul style="list-style-type: none"> <li>• on – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller</li> </ul> </li> </ul> |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#show adoption offline
```

```
-----
          MAC                HOST-NAME          TYPE          RF-DOMAIN
-----
    00-15-70-88-9E-C4    br7131-889EC4    br7131        default
    11-22-33-44-55-66    br650-445566    br650         default
-----
```

```
Total number of APs displayed: 2
```

```
RFController(config-device-00-15-70-37-FA-BE)#
```

```
RFController(config-adoption-policy-test)#show adoption info
```

```
Number of APs adopted : 1
Number of AAPs adopted : 0
Available AP licenses : 49
Available AAP licenses : 50
Device in cluster      : No
Cluster state          : active
```



```
-----  
MAC                HOST-NAME    TYPE  VERSION  ADOPTED-BY    LAST-ADOPTION  
-----  
00-A0-F8-00-00-00 br650-000000 br650 5.1.0.0  00-15-70-37-FA-BE 2011-02-17  
-----  
Total number of APs displayed: 1  
RFController(config-adoption-policy-test)#  
  
RFController(config)#show adoption history  
-----  
MAC                TYPE      EVENT      REASON      TIME-STAMP  
-----  
00-23-68-13-9B-34 BR7131  adopted      N.A.        2011-01-01 05:28:14  
-----  
RFController(config)#
```

## advanced-wips

### *show commands*

Displays advanced-wips settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
show advanced-wips [configuration|stats]
show advanced-wips configuration [events {thresholds}|terminate-list]
show advanced-wips stats
[ap-table|connected-sensors|detected-aps{authorized|neighboring|
unauthorized}|detected-stations-for-ap
<AA-BB-CC-DD-EE-FF>{authorized|neighboring|unauthorized}|
event-history|server-listening-port|client-table]
```

## Parameters

|                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| configuration [events thresholds] terminate-list]                                                                                                                                                                                              | <p>Displays advanced WIPS configuration details</p> <ul style="list-style-type: none"> <li>events {thresholds} – Displays events summary             <ul style="list-style-type: none"> <li>thresholds – Displays thresholds details</li> </ul> </li> <li>terminate-list – Displays the terminate list</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| stats<br>[ap-table   connected-sensors   detected-aps{authorized   neighboring   unauthorized}   detected-stations-for-ap <AA-BB-CC-DD-EE-FF>{authorized   neighboring   unauthorized}   event-history   server-listening-port   client-table] | <p>Displays advanced WIPS statistics details</p> <ul style="list-style-type: none"> <li>ap-table – Displays the AP table</li> <li>connected-sensors – Displays connected sensors information</li> <li>detected-aps – Displays detected AP details             <ul style="list-style-type: none"> <li>authorized – Displays detected authorized AP information</li> <li>neighboring – Displays detected neighboring AP information</li> <li>unauthorized – Displays detected unauthorized AP information</li> </ul> </li> <li>detected-stations-for-ap – Displays detected clients for APs             <ul style="list-style-type: none"> <li>&lt;AA-BB-CC-DD-EE-FF&gt; – Enter the AP BSSID                 <ul style="list-style-type: none"> <li>authorized – Displays detected authorized AP information</li> <li>neighboring – Displays detected neighboring AP information</li> <li>unauthorized – Displays detected unauthorized AP information</li> </ul> </li> </ul> </li> <li>event-history – Displays the event history</li> <li>server-listening-port – Displays server listening port information</li> <li>client-table – Displays the station table</li> </ul> |

## Example

```
RFController(config)#show advanced-wips configuration events
```

| POLICY | SLNO | NAME                                        | AUTHORIZED | UNAUTHORIZED | NEIGHBORING |
|--------|------|---------------------------------------------|------------|--------------|-------------|
| test   | 1    | unauthorized-bridge                         | N          | N            | N           |
| test   | 2    | dos-eapol-logoff-storm                      | N          | N            | N           |
| test   | 3    | monkey-jack-attack-detected                 | N          | N            | N           |
| test   | 4    | dos-cts-flood                               | N          | N            | N           |
| test   | 5    | crackable-wep-iv-used                       | N          | N            | N           |
| test   | 6    | multicast-ospf-all-routers-detection        | N          | N            | N           |
| test   | 7    | rogue-ap-detection                          | N          | N            | N           |
| test   | 8    | fake-dhcp-server-detected                   | N          | N            | N           |
| test   | 9    | multicast-vrrp-agent                        | N          | N            | N           |
| test   | 10   | multicast-ospf-designated-routers-detection | N          | N            | N           |
| test   | 11   | multicast-rip2-routers-detection            | N          | N            | N           |
| test   | 12   | multicast-dhcp-server-relay-agent           | N          | N            | N           |
| test   | 13   | id-theft-out-of-sequence                    | N          | N            | N           |
| test   | 14   | stp-detection                               | N          | N            | N           |
| test   | 15   | invalid-management-frame                    | N          | N            | N           |
| test   | 16   | fata-jack-detected                          | N          | N            | N           |
| test   | 17   | dos-deauthentication-detection              | N          | N            | N           |
| test   | 18   | windows-zero-config-memory-leak             | N          | N            | N           |
| test   | 19   | dos-eap-failure-spoof                       | N          | N            | N           |
| test   | 20   | multicast-all-routers-on-subnet             | N          | N            | N           |
| test   | 21   | ssid-jack-attack-detected                   | N          | N            | N           |

## 7 show commands

|      |    |                                       |   |   |   |
|------|----|---------------------------------------|---|---|---|
| test | 22 | dos-rts-flood                         | N | N | N |
| test | 23 | accidental-association                | N | N | N |
| test | 24 | probe-response-flood                  | N | N | N |
| test | 25 | invalid-channel-advertized            | N | N | N |
| test | 26 | id-theft-eapol-success-spoof-detected | N | N | N |
| test | 27 | multicast-igmp-detection              | N | N | N |
| test | 28 | netbios-detection                     | N | N | N |
| test | 29 | ipx-detection                         | N | N | N |
| test | 30 | null-probe-response-detected          | N | N | N |
| test | 31 | multicast-igmp-routers-detection      | N | N | N |
| test | 32 | wlan-jack-attack-detected             | N | N | N |
| test | 33 | multicast-hsrp-agent                  | N | N | N |
| test | 34 | dos-disassociation-detection          | N | N | N |
| test | 35 | multicast-all-systems-on-subnet       | N | N | N |
| -    | -  | -                                     | N | N | N |

RFController(config)#

RFController(config)#show advanced-wips configuration events thresholds

| POLICY | # | EVENT                  | THRESHOLD              | VALUE |
|--------|---|------------------------|------------------------|-------|
| test   | 1 | dos-eapol-logoff-storm | eapol-start-frames-ap  | 9     |
| test   | 2 | dos-eapol-logoff-storm | eapol-start-frames-mu  | 99    |
| test   | 3 | dos-cts-flood          | cts-frames-ratio       | 8     |
| test   | 4 | dos-cts-flood          | mu-rx-cts-frames       | 20    |
| test   | 5 | probe-response-flood   | probe-rsp-frames-count | 50    |
| -      | - | -                      | -                      | -     |

RFController(config)#

RFController(config)#show advanced-wips stats detected-stations-for-ap

11-22-33-44-55-66 authorized

Number of stations associated to the AP 11-22-33-44-55-66: 0

RFController(config)#

RFController(config)#show advanced-wips stats client-table

Number of clients: 2

RFController(config)#

## ap-upgrade

### show commands

Displays Access Point software image upgrade information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show ap-upgrade [history|status {on rf-domain-manager}|versions {on
rf-domain-manager}]
```

### Parameters

---

|                                                                             |                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| history status {on<br>rf-domain-manager} versions<br>{on rf-domain-manager} | <ul style="list-style-type: none"> <li>• history – Displays the history of an AP</li> <li>• status – Displays the status of an AP</li> <li>• versions – Displays the list of available upgrade images on all the<br/>Controllers</li> </ul> |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#show ap-upgrade history
-----
AP                RESULT TIME                RETRIES LAST UPDATE ERR UPGRADED BY
-----
00-A0-F8-00-00-01 done Feb 22 08:44:09 2011 0      -      00-15-70-37-FA-BE
00-A0-F8-00-00-10 done Feb 05 05:20:14 2011 0      -      00-15-70-37-FA-BE
-----

RFController(config)#

RFController(config)#show ap-upgrade versions
-----
CONTROLLER                AP-TYPE                VERSION
-----
00-15-70-37-FA-BE                br650                5.1.0.0-012D
00-15-70-37-FA-BE                br7131                none
00-15-70-37-FA-BE                br6511                none
-----

RFController(config)#
```

## boot

### show commands

Displays the boot configuration of a device. Use the 'on' command to view the boot configuration on a remote device.

---

**NOTE**

This command is not present in the USER EXEC Mode.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
show boot {on <DEVICE-NAME>}
```

**Parameters**


---

|                         |                                                |
|-------------------------|------------------------------------------------|
| boot {on <DEVICE-NAME>} | Displays boot information of a selected device |
|-------------------------|------------------------------------------------|

---

**Example**

```
RFController(config)#show boot on RFController
+-----+-----+-----+-----+
| IMAGE | BUILD DATE | INSTALL DATE | VERSION |
+-----+-----+-----+-----+
| Primary | 03:26:2010 09:57:35 UTC | 04:01:2010 11:01:13 UTC | 5.1.0.0 |
| Secondary | 03:17:2010 04:19:10 UTC | 03:18:2010 16:41:44 UTC | 5.1.0.0 |
+-----+-----+-----+-----+
Current Boot      : Primary
Next Boot         : Primary
Software Fallback : Enabled
RFController(config)#
```

## captive-portal

### [show commands](#)

Displays WLAN hotspot information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show captive-portal client {filter/on}
show captive-portal client filter {captive-portal/ip/state/vlan/wlan}
show captive-portal client filter captive-portal {CAPTIVE-PORTAL/not
CAPTIVE-PORTAL}
show captive-portal client filter ip {<A.B.C.D>/not <A.B.C.D>}
show captive-portal client filter state [not[pending|success]
|pending|success]
show captive-portal client filter vlan [VLAN-ID|not VLAN-ID]
show captive-portal client filter wlan [WLAN|not WLAN]
show captive-portal client {on <DEVICE-OR-DOMAIN-NAME>} filter
{captive-portal/ip/state/vlan/wlan}
```

## Parameters

---

client {filter|on}

Displays connected captive portal client information

- filter {captive-portal|ip|state|vlan|wlan} – Specifies an additional selection filter for getting table values
- {on <DEVICE-OR-DOMAIN-NAME>} {filter {captive-portal|ip|state|vlan|wlan} – On AP/Controller or RF Domain name

The following are common for the above:

- captive-portal {CAPTIVE-PORTAL|not CAPTIVE-PORTAL} – Displays clients on the selected captive portal
    - CAPTIVE-PORTAL – Specify captive-portal name
    - not CAPTIVE-PORTAL – Invert match selection
  - ip {<A.B.C.D>|not <A.B.C.D>} – Selection by IP address
    - <A.B.C.D> – Specify IP address
    - not <A.B.C.D> – Invert match selection
  - state [not[pending|success] |pending|success] – Selection based on state
    - pending – Clients redirected for authentication
    - success – Clients successfully authenticated
    - not [pending|success] – Invert match selection
  - vlan [VLAN-ID|not VLAN-ID]– Displays clients on given VLAN
    - VLAN-ID – Specify the VLAN number
    - not VLAN-ID – Invert match selection
  - wlan [WLAN|not WLAN] – Displays clients on given WLAN
    - WLAN – Specify the WLAN name
    - not WLAN – Invert match selection
- 

## Example

```
RFController(config)#show captive-portal client on RFController
Number of Hotspot Mobile-Units: 1
```



## cdp

### show commands

Displays Cisco Discovery Protocol (CDP) neighbor table

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show cdp neighbors {on <DEVICE-NAME>}
```

### Parameters

---

|                              |                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| neighbors {on <DEVICE-NAME>} | Displays the CDP neighbor table                                                                                                                         |
|                              | <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt; } - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> </ul> |

---

### Example

```
RFController(config)#sh cdp neighbors on RFController
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
-----
DEVICE ID  LPORT  TTL   CAPABILITY           PLATFORM              PORT ID
-----
Switch     gel     170   R S I                cisco WS-C3560-24PS   FastEthernet0/2
-----
```

## clock

### [show commands](#)

Displays the software system clock

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show clock {on <DEVICE-NAME>}
```

### Parameters

---

|                          |                                         |
|--------------------------|-----------------------------------------|
| clock {on <DEVICE-NAME>} | • on – On AP/Controller                 |
|                          | • <DEVICE-NAME> – On AP/Controller name |

---

### Example

```
RFController(config)#show clock on RFController
Apr 09 13:49:48 UTC 2010
RFController(config)#
```

## cluster

### show commands

Displays cluster related information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show cluster [configuration|members|status]
```

### Parameters

---

|                                               |                                                                                                                                                                                                                                                        |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cluster [configuration members detail status] | <ul style="list-style-type: none"> <li>• configuration – Displays cluster configuration parameters</li> <li>• members detail – Displays known cluster members information in detail</li> <li>• status – Displays cluster status information</li> </ul> |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#show cluster configuration
Cluster Configuration Information
  Mode           : Active
  Number of peer(s) : 0
  Auto revert     : Disabled
  Auto revert interval (Mins) : 5
  Controller AP license : 0
  Controller AAP license : 0
  Controller max AP adoption capacity : 1024
```

```
Cluster Runtime Information
  Cluster protocol version : 1
  Cluster run state       : active
  Cluster AP license      : 0
  Cluster AAP license     : 0
  Controller AP count     : 0
  Controller AAP count    : 0
  Cluster AP count        : 0
  Cluster AAP count       : 0
  Cluster max AP adoption capacity : 1024
  Number of connected peer(s) : 0
```

```
RFController(config)#show cluster members detail
```

| ID          | MAC               | MODE   | APCNT | AAPCNT | APLICENSE | AAPLICENSE | VERSION |
|-------------|-------------------|--------|-------|--------|-----------|------------|---------|
| 70.37.fa.be | 00-15-70-37-FA-BE | Active | 0     | 0      | 0         | 0          | Unknown |

## commands

### [show commands](#)

Displays available commands for the current mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show commands
```

### Parameters

None

### Example

```
RFController(config)#show commands
  help
  help search WORD (|detailed|only-show|skip-show)
  show commands
  show debugging (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging cfgd
  show debugging wireless (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging voice (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging captive-portal (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging dhcpsvr (|(on DEVICE-NAME))
  show debugging mstp (|(on DEVICE-OR-DOMAIN-NAME))
  show debugging advanced-wips
  show debugging vpn (|(on DEVICE-NAME))
  show debugging radius (|(on DEVICE-NAME))
  show (running-config|session-config) (|include-factory)
  show running-config interface (|`WORD|ge <1-4>|me1|pc <1-4>|vlan <1-4094>')
(|include-factory)
  show running-config wlan WLAN (|include-factory)
  show (running-config) device (self|DEVICE-NAME) (|include-factory)
  show session-changes
  show startup-config (|include-factory)
  show adoption info (|(on DEVICE-NAME))
  show adoption offline
  show licenses
  show password-encryption status
  show debug xpath get WORD (|WORD)
  show debug xpath count WORD
  show debug xpath list WORD
  show rf-domain-manager
  show timezone
  show event-history
  show ntp status
```

```
show ntp associations (|detail)
show device-categorization summary
show wireless ap (|(on DEVICE-OR-DOMAIN-NAME))
show wireless ap configured
show wireless ap detail (|WORD)
show wireless unsanctioned aps (|(on DEVICE-OR-DOMAIN-NAME))
show wireless unsanctioned aps detailed (|(on DEVICE-OR-DOMAIN-NAME))
show wireless unsanctioned aps statistics (|(on DEVICE-OR-DOMAIN-NAME))
show wireless client (|(on DEVICE-OR-DOMAIN-NAME)) (|(filter {(state (|not)
(data-ready|roaming))|(wlan (|not) WLAN)|(ip (|not) A.B.C.D)}))
show wireless client detail AA-BB-CC-DD-EE-FF (|(on DEVICE-OR-DOMAIN-NAME))
show wireless client statistics (|traffic) (|(on DEVICE-OR-DOMAIN-NAME))
show wireless client statistics rf (|(on DEVICE-OR-DOMAIN-NAME))
.....
RFController(config)#
```

## context

### [show commands](#)

Displays information about the current context

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show context {include-factory|session-config {include-factory}}
```

### Parameters

---

|                                                          |                                                                                                                                                                                               |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| context {include-factory session-config include-factory} | <ul style="list-style-type: none"> <li>• include-factory – Displays information (including factory default values)</li> <li>• session-config – Displays running system information</li> </ul> |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFCcontroller(config)#show context include-factory
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
no enable
auto-assign detector
auto-assign channel
auto-assign power
assignable-power 5Ghz min 1
assignable-power 5Ghz max 20
assignable-power 2.4Ghz min 1
assignable-power 2.4Ghz max 20
channel-list 5Ghz
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,1
57,161,165
channel-list 2.4Ghz 1,6,11
channel-width 5Ghz 40Mhz
channel-width 2.4Ghz 20Mhz
smart-ocs-monitoring
smart-ocs-monitoring off-channel-duration 5Ghz 50
smart-ocs-monitoring off-channel-duration 2.4Ghz 50
smart-ocs-monitoring frequency 5Ghz 6
smart-ocs-monitoring frequency 2.4Ghz 6
smart-ocs-monitoring sample-count 5Ghz 5
```

```
smart-ocs-monitoring sample-count 2.4Ghz 5
smart-ocs-monitoring extended-scan-frequency 5Ghz 5
smart-ocs-monitoring extended-scan-frequency 2.4Ghz 5
interference-recovery
interference-recovery noise
interference-recovery interference
no interference-recovery retry-threshold
interference-recovery channel-Controller-delta 5Ghz 20
interference-recovery .....
RFController(config)#

RFController(config)#show context session-config
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
enable
calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
voice-prioritization
svp-prioritization
wmm background cw-max 8
wmm video txop-limit 9
wmm voice cw-min 6
wmm voice cw-max 6
rate-limit client to-air max-burst-size 3
rate-limit client to-air red-threshold video 101
rate-limit client from-air rate 55
rate-limit client from-air max-burst-size 6
rate-limit client from-air red-threshold background 100
rate-limit client from-air red-threshold voice 1010
!.....
RFController(config)#
```

## critical-resources

### show commands

Displays critical resource information. Critical resources are resources that are vital to the wellbeing of the controller managed network.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show critical-resources {on <DEVICE-NAME>}
```

### Parameters

---

|                                          |                                                                                                                                  |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| critical-resources {on<br><DEVICE-NAME>} | Displays critical resource information                                                                                           |
|                                          | <ul style="list-style-type: none"> <li>• on – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> |

---

### Example

```
RFController(config)#sh critical-resources on RFController
-----
CRITICAL RESOURCE IP          VLAN          PING-MODE          STATE
-----
172.168.1.103              1              arp-icmp            up
```



## crypto

### show commands

Displays encryption mode information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show crypto [ipsec|isakmp|key|pki]
show crypto [ipsec|isakmp] sa {on <DEVICE-NAME>}
show crypto key rsa {on <DEVICE-NAME>|public-key-detail {on <DEVICE-NAME>}}
show crypto pki trustpoints {<WORD> {on <DEVICE-NAME>}}|all {on
<DEVICE-NAME>}|on <DEVICE-NAME>}
```

### Parameters

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ipsec isakmp] sa {on <DEVICE-NAME>}                                                 | <ul style="list-style-type: none"> <li>• ipsec – Displays the IPSEC policy</li> <li>• isakmp – Displays the ISAKMP policy</li> </ul>                                                                                                                                                                                                                                                                                                                                                                   |
| The following parameters are common for the above:                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                                                      | <ul style="list-style-type: none"> <li>• sa – All crypto ISAKMP security associations <ul style="list-style-type: none"> <li>• on – Displays ISAKMP security associations on AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays AP/Controller name</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                               |
| key rsa {on <DEVICE-NAME> public-key-detail {on <DEVICE-NAME>}}                      | Displays key management operations <ul style="list-style-type: none"> <li>• rsa – Displays RSA public keys <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – On AP/Controller</li> <li>• public-key-detail {on} &lt;DEVICE-NAME&gt; – Displays the public key in PEM format <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays the AP/Controller name</li> </ul> </li> </ul> </li> </ul>                                                                          |
| pki trustpoints {<WORD> {on <DEVICE-NAME>}} all {on <DEVICE-NAME>} on <DEVICE-NAME>} | Displays Public Key Infrastructure related commands <ul style="list-style-type: none"> <li>• trustpoints – Displays configured trustpoints <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Displays a particular trustpoint's information in detail</li> <li>• all – Displays details for all trustpoints</li> <li>• {on} &lt;DEVICE-NAME&gt; – On AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays AP/Controller name</li> </ul> </li> </ul> </li> </ul> |

**Example**

```
RFController(config)#show crypto key rsa public-key-detail on RFController
```

```
RSA key name: default-trustpoint-srvr-priv-key   Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGHBR2bxLeRZ4G6hm7jHJRSaeE
A216r4s4qptiSld+rKeMihPTFbYELeDk3dITkzF1EU7Ov0vKzant0pyAmdJ8ci//
wSQMmZjX3RwF9OFBRp2C09LFj/1VX2fsoD6xXhJHBLieJ9qzF+ZQ2CYG7+r29P/o
3rfr/GLaTN3C6RIWvQIDAQAB
-----END PUBLIC KEY-----
```

```
RSA key name: default_rsa_key                   Key-length: 1024
-----BEGIN PUBLIC KEY-----
MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQCwXXWGE9j/i3EiSjnY9x1Ktsbt
rzgqB1KhlShWignWqlxjzvO6SvGmBPG5XqBS3rKqIzrgh6fXF2cNJZweWgc1QktL
AoZN/MeCiGVGiJZmtmyKihPMGyyLGqm6krvWFfOdqlA85+WdQyvDsevTVVp/OiEB
al4SsIvMG+U+UQaIlwIBIw==
-----END PUBLIC KEY-----
```

```
RFController(config)#
```

```
RFController(config)#show crypto key rsa on RFController
```

| # | KEY NAME                         | KEY LENGTH |
|---|----------------------------------|------------|
| 1 | default-trustpoint-srvr-priv-key | 1024       |
| 2 | default_rsa_key                  | 1024       |

```
RFController(config)#
```

```
RFController(config)#show crypto pki trustpoints all on RFController
```

```
Trustpoint Name: default-trustpoint           (self signed)
```

```
-----
CRL present: no
Server Certificate details:
  Key used: default-trustpoint-srvr-priv-key
  Serial Number: 0671
  Subject Name:
    C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EMLAN, CN=Brocade
  Issuer Name:
    C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EMLAN, CN=Brocade
  Valid From : Tue Sep 22 16:19:51 2009 UTC
  Valid Until: Wed Sep 22 16:19:51 2010 UTC
```

```
RFController(config)#
```

```
RFController(config)#show crypto pki trustpoints all
```

```
Trustpoint Name: default-trustpoint           (self signed)
```

```
-----
CRL present: no
Server Certificate details:
  Key used: default-trustpoint-srvr-priv-key
  Serial Number: 0671
```

```
Subject Name:
  C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Brocade
Issuer Name:
  C=US, ST=CA, L=San Jose, O=Enterprise Mobility, OU=EWLAN, CN=Brocade
Valid From : Tue Sep 22 16:19:51 2009 UTC
Valid Until: Wed Sep 22 16:19:51 2010 UTC
```

```
RFController(config)#
RFController(config)#show crypto pki trustpoints
+-----+-----+-----+
|TRUSTPOINT      | KEY NAME                               |VALID UNTIL      |
+-----+-----+-----+
default-trustpoint|default-trustpoint-srvr-priv-key|Wed Sep 22 16:19:51 2010UTC|
+-----+-----+-----+
RFController(config)#
```

## debug

### show commands

Displays debugging configuration information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show debug [profile|xpath]
show debug profile <WORD> {arg <WORD>}
show debug xpath [count|get|list]
show debug xpath [count|list] <WORD>
show debug xpath get <WORD> {option|param <WORD>} [do-profiling|
no-pretty|show-tail-only|use-streaming] {do-profiling|
no-pretty|show-tail-only|use-streaming}
```

### Parameters

---

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| profile <WORD> {arg <WORD>} | <p>Displays profile functions debugging information</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the function name.</li> <li>• arg &lt;WORD&gt; – Specify arguments for the function in a single word, separated by a comma ( e.g., _cli,[3,4])</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| xpath [count get list]      | <p>Displays xpath based operations debugging information</p> <ul style="list-style-type: none"> <li>• count &lt;WORD&gt; – Prints the number of items under an xpath node</li> <li>• list &lt;WORD&gt; – Lists the names (keys) under an xpath node</li> <li>• get &lt;WORD&gt; {option param &lt;WORD&gt;} [do-profiling no-pretty show-tail-only use-streaming] – Prints the value of an xpath node based on option or parameters <ul style="list-style-type: none"> <li>• option – Specify options for the debug command</li> <li>• param &lt;WORD&gt; – Specify parameters for the xpath <ul style="list-style-type: none"> <li>• do-profiling – Performs profiling</li> <li>• no-pretty – Disables pretty for speed</li> <li>• show-tail-only – Displays only the tail of the result</li> <li>• use-streaming – Uses streaming interface</li> </ul> </li> </ul> </li> </ul> |

---

**Example**

```

RFController(config)#show debug xpath count /wing-stats
Success: 4
RFController(config)#

RFController(config)#show debug xpath get word option do-profiling no-pretty
Sun Dec  5 08:52:08 2010    /var/profile

                26 function calls in 0.001 CPU seconds

Ordered by: standard name

ncalls  tottime  percall  cumtime  percall  filename:lineno(function)
  1     0.000   0.000   0.001    0.001  <string>:1(<module>)
  1     0.000   0.000   0.001    0.001
cluster_db_api.py:20(cluster_db_get_api)
  1     0.000   0.000   0.001    0.001
debugcli.py:150(debug_xpath_get_stats_body)
  2     0.000   0.000   0.000    0.000  log.py:133(dlog)
  1     0.000   0.000   0.000    0.000  re.py:144(sub)
  1     0.000   0.000   0.000    0.000  re.py:227(_compile)
  1     0.000   0.000   0.000    0.000  utils.py:147(dlog_stats)
  1     0.000   0.000   0.000    0.000  utils.py:159(dlog_snmp)
  1     0.000   0.000   0.000    0.000  xpath_parser.py:104(__init__)
  1     0.000   0.000   0.000    0.000  xpath_parser.py:124(splitsegments)
  1     0.000   0.000   0.000    0.000  xpath_parser.py:194(stripFilters)
  1     0.000   0.000   0.000    0.000  xpath_parser.py:6(__init__)
  1     0.000   0.000   0.000    0.000  {built-in method sub}
  1     0.000   0.000   0.000    0.000  {isinstance}
  2     0.000   0.000   0.000    0.000  {len}
  2     0.000   0.000   0.000    0.000  {method 'append' of 'list' objects}
  1     0.000   0.000   0.000    0.000  {method 'disable' of
'_lsprof.Profiler' objects}
  1     0.000   0.000   0.000    0.000  {method 'find' of 'str' objects}
  3     0.000   0.000   0.000    0.000  {method 'get' of 'dict' objects}
  2     0.000   0.000   0.000    0.000  {method 'startswith' of 'str' objects}
done profiling
RFController(config)#

RFController(config)#show debug xpath list /wing-stats
Success: ['cluster', 'device', 'rf_domain', 'noc']
RFController(config)#

```

## debugging

### *show commands*

Displays debugging configuration information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
show debugging {advanced-wips/captive-portal/cfgd/dhcpsvr/mstp/nsm/on/  
radius/snmp/voice/vpn/wireless}  
show debugging advanced-wips  
show debugging {captive-portal/dhcpsvr/mstp/nsm/radius/voice/vpn/wireless}  
{on <DEVICE-OR-DOMAIN-NAME>}  
show debugging {on <DEVICE-OR-DOMAIN-NAME>}  
show debugging snmp {on <DEVICE-NAME>}
```

## Parameters

debugging {advanced-wips | captive-portal |  
cfgd | dhcpsvr | mstp | on | radius | voice | vpn | wireless}

Displays debugging functions:

- captive-portal – Displays the debugging configuration of a hotspot (HSD) module
- mstp – Displays the debugging configuration of a Multiple Spanning Tree (MST) module
- nsm – Displays the debugging configuration of *Network Service Module (NSM)*
- voice – Displays the debugging configuration of a voice module
- wireless – Displays the debugging configuration of a wireless module
- cfgd – Displays debugging information of a Cfgd process
- dhcpsvr – Displays debugging information of a DHCP server configuration module
- RADIUS – Displays debugging information for a radius configuration module
- vpn – Displays debugging information for a VPN module
- snmp {on <DEVICE-NAME>} – Displays the debugging configuration of SNMP module
- {on <DEVICE-NAME>} – On AP/Controller
  - <DEVICE-NAME> – On AP/Controller name

The following parameters are common for all the above except advanced-wips:

- on – On AP/Controller or RF Domain
  - <DEVICE-OR-DOMAIN-NAME> – AP/Controller/RF-Domain name
- advanced-wips – Displays the debugging configuration of Advanced-WIPS module

## Example

```
RFController(config)#show debugging mstp on RFController
RFController(config)#
```

```
RFController(config-critical-resource-policy-test)#show debugging vpn on
RFController
RFController(config-critical-resource-policy-test)#
```

```
RFController(config-critical-resource-policy-test)#show debugging radius on
RFController
RFController(config-critical-resource-policy-test)#
```

## device-categorization

### show commands

Displays device categorization details

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show device-categorization summary
```

### Parameters

|         |                                          |
|---------|------------------------------------------|
| summary | Displays a device categorization summary |
|---------|------------------------------------------|

### Example

```
RFController(config)#show device-categorization summary
```

```
-----
POLICY                #      A/N      AP/CLIENT  MAC          SSID
-----
DEVICE-CATEGORIZATION 1  sanctioned  client  00-40-96-B0-BA-2D  -
DEVICE-CATEGORIZATION 2  neighboring  client  00-40-96-B0-BA-2A  -
DEVICE-CATEGORIZATION 3  sanctioned   ap     00-23-68-31-12-65  ASDF
-----
```

```
RFController(config)#
```



## event-history

### show commands

Displays an event history

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show event-history {on <DEVICE-NAME>}
```

### Parameters

- 
- |                    |                                         |
|--------------------|-----------------------------------------|
| {on <DEVICE-NAME>} | • on <DEVICE-NAME> - On AP/Controller   |
|                    | • <DEVICE-NAME> - On AP/Controller name |
- 

### Example

```
RFController(config)#show event-history
Wed Apr  7 18:16:06 2010 00-15-70-37-FA-BE NO_COUNTRY_CODE Country-code
not set in configuration. Radio operations disabled
RFController(config)#

RFController(config)#show event-history on RFController
2011-01-05 08:44:30      00-15-70-37-FA-BE SYSTEM      LOGOUT
Logged out User: 'admin' with privilege 'superuser' from '172.16.10.10'
2011-01-05 08:39:30      00-15-70-37-FA-BE SYSTEM      LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2011-01-05 08:38:57      00-15-70-37-FA-BE SYSTEM      LOGOUT
Logged out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2011-01-05 08:25:31      00-15-70-37-FA-BE SYSTEM      LOGOUT
Logged out User: 'admin' with privilege 'superuser' from '172.16.10.10'
2011-01-05 08:23:34      00-15-70-37-FA-BE SYSTEM      LOGOUT
Logged out User: 'admin' with privilege 'superuser' from '172.16.10.12'
2011-01-05 08:21:09      00-15-70-37-FA-BE SYSTEM      LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2011-01-05 08:20:42      00-15-70-37-FA-BE SYSTEM      LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
2011-01-05 05:35:35      00-15-70-37-FA-BE SYSTEM      LOGIN
Successfully logged in User: 'admin' with privilege 'superuser' from 'ssh'
-----
Country of operation configured to IN [India]
RFController(config)#
```

## event-system-policy

### show commands

Displays event system policy configuration information in detail

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show event-system-policy [config|detail] <EVENT-SYSTEM-POLICY>
```

### Parameters

---

|                       |                                                                                 |
|-----------------------|---------------------------------------------------------------------------------|
| [config detail]       | • config - Displays configuration information for the selected policy           |
| <EVENT-SYSTEM-POLICY> | • detail - Displays configuration information for the selected policy in detail |
|                       | • <EVENT-SYSTEM-POLICY> - Specify the event system policy name                  |

---

### Example

```
RFController(config)#show event-system-policy config testpolicy
-----
MODULE          EVENT          SYSLOG  SNMP  FORWARD  EMAIL
-----
aaa             radius-discon-msg  on      on    on        default
-----
RFController(config)#

RFController(config)#show event-system-policy detail testpolicy
-----
MODULE  EVENT          SYSLOG  SNMP  FORWARD  EMAIL
-----
aaa     radius-discon-msg      on      on    on        default
aaa     radius-session-expired default  default default default
aaa     radius-session-not-started default default default default
aaa     radius-vlan-update     default default default default
adv-wips adv-wips-event-1      default default default default
```

## file

### [show commands](#)

Displays file system information

---

#### NOTE

This command is not present in USER EXEC Mode

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
show file [information <FILE>|systems]
```

---

#### Parameters

- |                              |                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [information <FILE> systems] | <ul style="list-style-type: none"> <li>• information &lt;FILE&gt; – Displays file system information             <ul style="list-style-type: none"> <li>• &lt;FILE&gt; – Displays information for a specified file</li> </ul> </li> <li>• systems – Displays the list of file systems present in the system</li> </ul> |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

#### Example

```
RFController(config)#show file systems
File Systems:

      Size(b)      Free(b)      Type  Prefix
      -          -          -     -
      10485760     9916416     flash nvram:
      20971520     20131840     flash flash:
      -           -          network (null)
      -           -          network rdp:
      -           -          network sftp:
      -           -          network http:
      -           -          network ftp:
      -           -          network tftp:
      20971520     20131840     -     hotspot:
RFController(config)#
```

## firewall

### show commands

Displays wireless firewall information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show firewall [dhcp snoop-table|dos stats|flows]{on <DEVICE-NAME>}]
show firewall flows {filter/management/on <DEVICE-NAME>|stats/wireless-client
<MAC>}

show firewall flows filter {dir/dst port <1-65535>/ether[dst <MAC>/host
<MAC>/src <MAC>/vlan <1-4095>]|flow-type [bridge/natted/routed/
wired/wireless]/icmp {code/type}/igmp/ip[dst <IP>/proto <0-254>/host <IP>
{and}/src]/max-idle/min-bytes/min-pkts/not/port/src <IP> {and}/tcp/udp}
show firewall flows filter dir [wired-wired|
wired-wireless|wireless-wired|wireless-wireless]
{dst/ether/flow-type/ip/max-idle/min-bytes/
min-pkts/port/src}
show wireless flows filter ether vlan <1-4095> {and|dst/ether/
flow-type/ip/max-idle/min-bytes/min-pkts/port/src/src}

show firewall flows {management/stats} {on <DEVICE-NAME>}
```

## Parameters

---

- dhcp snoop-table | dos  
stats | flows ](on  
<DEVICE-NAME>}
- dhcp snoop table – Displays DHCP snoop-table entries
  - dos stats – Displays a list of statistics denied from service
  - flows {filter | management | on <DEVICE-NAME> | stats | wireless-client <MAC>} – Displays that a session has been established
    - filter dir | dst port <1-65535> | ether [dst <MAC> | host <MAC> | src <MAC> | vlan <1-4095>] | flow-type [bridge | natted | routed | wired | wireless] | icmp {code | type} | igmp | ip [dst <IP> | proto <0-254> | host <IP> {and} | src] | max-idle | min-bytes | min-pkts | not | port | src <IP> {and} | tcp | udp] – Displays filter parameters
      - dir [wired-wired | wired-wireless | wireless-wired | wireless-wireless] – Matches flow direction
        - wired-wired – Wired to wired flows
        - wired-wireless – Wired to wireless flows
        - wireless-wired – Wireless to wired flows
        - wireless-wireless – Wireless to wireless flows
      - dst – Matches only destination port
      - ether [dst <MAC> | host <MAC> | src <MAC> | vlan <1-4095>] – Displays ethernet parameters
        - dst – Matches only destination MAC address
        - host – Matches flows containing MAC address
        - src – Matches only source MAC address
        - vlan <1-4094> – Matches the VLAN of the traffic
      - flow-type [bridge | natted | routed | wired | wireless] – Matches the flow type
        - bridged – Bridged flows
        - natted – Natted flows
        - routed – Routed flows
        - wired – Flows belonging to wired hosts
        - wireless – Flows containing a mobile unit
      - icmp {code | type} – Matches flows with given ICMP code and ICMP type

- 
- [
  - igmp – Matches IGMP flows
  - ip [dst <IP> | proto <0-254> | host <IP> | src] – Displays IP V4 parameters
    - dst <IP> – Matches destination IP address
    - host <IP> – Matches flows containing IPv4 address
    - proto <0-254> – Matches the IPv4 protocol
    - src <IP> – Matches source IP address
- 
- max-idle – Matches flows which are idle atmost for the given duration
  - min-bytes – Matches flows which has seen atleast the given number of bytes
  - min-idle – Matches flows which are idle atleast for the given duration
  - min-pkts – Matches flows with at least the given number of packets
  - not – Negates the Filter Expression
  - port <1-65535> – Matches either source or destination port
  - src port <1-65535> – Matches only source port
  - tcp – Matches TCP flows
  - udp – Matches UDP flows
  - management on <DEVICE-NAME> – Displays firewall flows for management traffic
  - stats on <DEVICE-NAME> – Displays summary of active sessions
  - on – On AP/Controller
    - <DEVICE-NAME> – On AP/Controller name
  - wireless-client <MAC> – Displays firewall flows for wireless clients
- 

**Example**

```
RFController(config)#show firewall dhcp snoop-table on RFController
Snoop Binding <157.235.208.252, 00-15-70-37-FA-BE, Vlan 4>
Type Controller-SVI, Touched 32 seconds ago
-----
Snoop Binding <172.16.10.2, 00-15-70-37-FA-BE, Vlan 1>
Type Controller-SVI, Touched 1 seconds ago
-----
RFController(config)#
```

```
RFController(config)#show firewall dos stats on RFController
```

| ATTACK TYPE         | COUNT | LAST OCCURENCE |
|---------------------|-------|----------------|
| udp-short-hdr       | 0     | Never          |
| tcp-xmas-scan       | 0     | Never          |
| ascend              | 0     | Never          |
| ftp-bounce          | 0     | Never          |
| tcp-null-scan       | 0     | Never          |
| bcast-mcast-icmp    | 0     | Never          |
| fraggle             | 0     | Never          |
| router-advt         | 0     | Never          |
| tcp-post-syn        | 0     | Never          |
| winnuke             | 0     | Never          |
| tcp-header-fragment | 0     | Never          |
| tcp-ip-ttl-zero     | 0     | Never          |
| invalid-protocol    | 0     | Never          |
| icmp-router-solicit | 0     | Never          |
| tcp-intercept       | 0     | Never          |

|                  |   |       |
|------------------|---|-------|
| twinge           | 0 | Never |
| land             | 0 | Never |
| spoof            | 0 | Never |
| source-route     | 0 | Never |
| tcp-bad-sequence | 0 | Never |
| tcp-fin-scan     | 0 | Never |
| snork            | 0 | Never |
| chargen          | 0 | Never |
| smurf            | 0 | Never |

```
RFController(config)#
```

```
RFController(config)#show firewall flows brief on RFController
```

```
Active Flows      7
TCP flows        3
UDP flows        2
DHCP flows       0
ICMP flows       0
IPsec flows      0
L3/Unknown flows 2
RFController(config)#
```

```
RFController(config)#show firewall flows management on RFController
```

```
===== Flow# 1 Summary =====
```

```
Forward:
```

```
Vlan 1, TCP 172.16.10.10 port 3995 > 172.16.10.1 port 22
00-02-B3-28-D1-55 > 00-15-70-37-FA-BE, ingress port gel
Egress port: <local>, Egress interface: vlan1, Next hop: <local>
(00-15-70-37-FA-BE)
573 packets, 49202 bytes, last packet 0 seconds ago
```

```
Reverse:
```

```
Vlan 1, TCP 172.16.10.1 port 22 > 172.16.10.10 port 3995
00-15-70-37-FA-BE > 00-02-B3-28-D1-55, ingress port local
Egress port: gel, Egress interface: vlan1, Next hop: 172.16.10.10
(00-02-B3-28-D1-55)
552 packets, 63541 bytes, last packet 0 seconds ago
```

```
TCP state: Established
```

```
Flow times out in 1 hour 30 minutes
```

```
RFController(config)#
```

```
RFController(config)#show firewall flows stats on RFController
```

```
Active Flows      2
TCP flows        1
UDP flows        0
DHCP flows       1
ICMP flows       0
IPsec flows      0
L3/Unknown flows 0
RFController(config)#
```

## interface

### show commands

Displays the status of the different controller interfaces

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show interfaces [<WORD>|brief|counters|ge|me1|on|pc||switchport|vlan] {on
<DEVICE-NAME>}
```

### Parameters

|                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interfaces<br>[<WORD> brief counters ge m<br>e1 on pc  Controllerport vlan]<br>{on <DEVICE-NAME>} | <p>Displays the interface name</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Displays the interface name</li> <li>• brief - Displays a brief summary of interface status and configuration</li> <li>• ge &lt;1-4&gt; - Displays the configured Gigabit Ethernet interface status</li> <li>• me1 - Displays the Fast Ethernet interface status</li> <li>• counters - Displays interface TX/RX counters</li> <li>• on - Displays information on AP/controller</li> <li>• pc &lt;1-4&gt; - Displays port-channel information</li> <li>• Controllerport - Displays the status of layer2 interfaces</li> <li>• vlan &lt;1-4094&gt; - Displays configured vlan information</li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• on - Displays information on AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - Displays information on the AP/Controller/RF Domain name</li> </ul> </li> </ul> |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Example

```
RFController(config)#show interface Controllerport on RFController
+-----+-----+-----+-----+
| INTERFACE | STATUS | MODE | VLAN(S) |
+-----+-----+-----+-----+
ge3	DOWN	access	1
ge2	UP	access	1
ge1	UP	access	1
ge4	DOWN	access	1
+-----+-----+-----+-----+
A '*' next to the VLAN ID indicates the native vlan for that trunk port
RFController(config)#
```

```
RFController(config)#show interface vlan 1
Interface vlan1 is UP
Hardware-type: vlan, Mode: Layer 3, Address: 00-15-70-37-FA-BE
```



```

Index: 4, Metric: 1, MTU: 1500
IP-Address: 172.16.10.2/24
  input packets 34801, bytes 5380250, dropped 0, multicast packets 0
  input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
  output packets 7848, bytes 6847627, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
  collisions 0

```

```
RFController(config)#
```

```
RFController(config)#show interface ge 2 on RFController
```

```

Interface ge2 is UP
  Hardware-type: ethernet, Mode: Layer 2, Address: 00-15-70-37-FA-C0
  Index: 2002, Metric: 1, MTU: 1500
  Speed: Admin Auto, Operational 100M, Maximum 1G
  Duplex: Admin Auto, Operational Full
  Active-medium: Copper
  Controllerport settings: access, access-vlan: 1
    Input packets 6, bytes 620, dropped 0
    Received 0 broadcasts, 6 multicasts
    Input errors 0, runts 0, giants 0
    CRC 0, frame 0, fragment 0, jabber 0
    Output packets 45524, bytes 8708231, dropped 0
    Sent 21302 broadcasts, 22261 multicasts
    Output errors 0, collisions 0, late collisions 0
    Excessive collisions 0

```

```
RFController(config)#
```

```
RFController(config)#show interface counters
```

```

-----
|INTERFACE|  MAC  |RX-PKTS| RX-BYTES|RX-DROPPED|TX-PKTS|TX-BYTES|TX-DROPPED|
-----
ge3	00-15-70-37-FA-C1	0	0	0	46592	8946900	0
ge2	00-15-70-37-FA-C0	6	620	0	46582	8914407	0
ge1	00-15-70-37-FA-BF	56429	9384360	0	18047	12019031	0
ge4	00-15-70-37-FA-C2	0	0	0	46592	8946900	0
me1	00-15-70-CC-5E-F7	0	0	0	0	0	0
vlan44	00-15-70-37-FA-BE	0	0	0	0	0	0
vlan1	00-15-70-37-FA-BE	6471	7221803	0	9875	9106192	0
vlan4	00-15-70-37-FA-BE	0	0	0	0	0	0
-----

```

## ip

### show commands

Displays Internet Protocol (IP) related information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

show ip
[arp|ddns|dhcp|dhcp-vendor-options|domain-name|igmp|interface|name-server|nat
|route|routing]
show ip arp {<VLAN Name> {on <DEVICE-NAME>}/on <DEVICE-NAME>}

show ip ddns bindings {on <DEVICE-NAME>}

show ip dhcp [bindings|networks|status]
show ip dhcp bindings {on <DEVICE-NAME>/manual
{on <DEVICE-NAME>}}
show ip dhcp networks {on <DEVICE-NAME>}
show ip dhcp status {on <DEVICE-NAME>}
show ip [dhcp-vendor-options|domain-name|routing] {on <DEVICE-NAME>}
show ip igmp snooping [mrouter|vlan]
show ip igmp snooping mrouter vlan <1-4095> {on <DEVICE-NAME>}
show ip igmp snooping vlan <1-4095> {<A.B.C.D>/on}
show ip igmp snooping vlan <1-4095> {on <DEVICE-NAME>/<A.B.C.D> {on
<DEVICE-NAME>}}

show ip interface {<word>/brief/on}
show ip interface <word> {on <DEVICE-NAME>}
show ip interface brief {on <DEVICE-NAME>}
show ip interface {on <DEVICE-NAME>}

show ip nat translations verbose {on <DEVICE-NAME>}

show ip route {<WORD>/ge/me1/on/pc/vlan}
show ip route <WORD> {on <DEVICE-NAME>}
show ip route ge <1-4> {on <DEVICE-NAME>}
show ip route me1 {on <DEVICE-NAME>}
show ip route {on <DEVICE-NAME>}
show ip route pc <1-4> {on <DEVICE-NAME>}
show ip route vlan <1-4094> {on <DEVICE-NAME>}

```

## Parameters

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| arp {<VLAN Name> {on <DEVICE-NAME>} on <DEVICE-NAME>}        | <p>Displays the ARP configuration</p> <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the vlan name           <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller               <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller               <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ddns bindings {on <DEVICE-NAME>}                             | <p>Displays the DDNS configuration</p> <ul style="list-style-type: none"> <li>• bindings {on &lt;DEVICE-NAME&gt;} – DNS address bindings           <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller               <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| dhcp<br>[bindings   networks   status]<br>{on <DEVICE-NAME>} | <p>Displays the DHCP server configuration</p> <ul style="list-style-type: none"> <li>• bindings {on &lt;DEVICE-NAME&gt; manual {on &lt;DEVICE-NAME&gt;} – DNS address bindings           <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller               <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> <li>• manual – Displays static DHCP address bindings               <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller                   <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> </ul> </li> <li>• networks {on &lt;DEVICE-NAME&gt;} – Network information           <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller               <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> <li>• status {on &lt;DEVICE-NAME&gt;} – Displays status information           <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller               <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> </ul> |
| igmp snooping [mrouter   vlan]                               | <p>Displays <i>Internet Group Management Protocol (IGMP)</i> information</p> <ul style="list-style-type: none"> <li>• snooping – IGMP snooping           <ul style="list-style-type: none"> <li>• mrouter vlan &lt;1-4095&gt; {on &lt;DEVICE-NAME&gt;} – Multicast router               <ul style="list-style-type: none"> <li>• vlan &lt;1-4095&gt; – Specifies a VLAN index value from 1 and 4095                   <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> <li>• vlan &lt;1-4095&gt; {on &lt;DEVICE-NAME&gt; &lt;A.B.C.D&gt; {on &lt;DEVICE-NAME&gt;} – Specifies a VLAN index value from 1 and 4095               <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} – Displays information on the AP/Controller                   <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |

---

`interface {<WORD>|brief|on}` Use the show ip interface command to display the administrative and operational status of all Layer-3 interfaces or a specified Layer-3 interface.

- <WORD> – Interface name
- brief – Brief summary of the IP status and its configuration

The following parameters are common for the above.

- {on <DEVICE-NAME>} – Displays information on the AP/Controller
  - <DEVICE-NAME> – Displays information on the AP/Controller name
- on – Displays information on AP/controller
  - <DEVICE-NAME>} – Displays information on the AP/Controller name

---

`nat translations verbose {on <DEVICE-NAME>}` Displays *Network Address Translation (NAT)* information

- translations – Displays NAT translations
- verbose – Displays NAT Translations in real-time
  - on <DEVICE-NAME>} – Displays information on the AP/Controller
  - <DEVICE-NAME>} – Displays information on the AP/Controller/RF Domain name

---

`route {<WORD>|ge|me1|on|pc|vlan}` Displays route table information

- <WORD> – Interface name
- ge <1-4> – Displays the configured Gigabit Ethernet interface status
- me1 – Displays the FastEthernet interface status
- pc <1-4> – Displays information on the AP/controller
- Controllerport – Displays the status of layer2 interfaces
- vlan <1-4094> – Displays configured VLAN information

The following parameters are common for the above:

- {on} – Displays information on AP/Controller
  - <DEVICE-NAME> – Displays information on the AP/Controller name
- on <DEVICE- NAME> – Displays information on the AP/Controller
  - <DEVICE-NAME> – Displays information on the AP/Controller name

---

**Example**

```
RFController(config)#show ip arp test on RFController
```

| IP           | MAC               | INTERFACE | TYPE    |
|--------------|-------------------|-----------|---------|
| 172.16.10.11 | 00-50-DA-95-11-13 | vlan1     | dynamic |
| 172.16.10.10 | 00-02-B3-28-D1-55 | vlan1     | dynamic |

```
RFController(config)#
```

```
RFController(config)#show ip interface brief on RFController
```

| INTERFACE | IP-ADDRESS/MASK    | STATUS | PROTOCOL |
|-----------|--------------------|--------|----------|
| me1       | unassigned         | DOWN   | down     |
| vlan44    | unassigned         | UP     | up       |
| vlan1     | 172.16.10.2/24     | UP     | up       |
| vlan4     | 157.235.208.252/24 | UP     | up       |

```
RFController(config)#
```

```
RFController(config)#show ip nat translations verbose on RFController
```

```
PROTO ACTUAL SOURCE ACTUAL DESTINATION NATTED SOURCE NATTED DESTINATION
```

```
RFController(config)#
```

```
RFController(config)#show ip route test on RFController
```

```
+-----+-----+-----+-----+
| DESTINATION | GATEWAY | FLAGS | INTERFACE |
+-----+-----+-----+-----+
157.235.208.0/24	direct	C	vlan4
172.16.10.0/24	direct	C	vlan1
default	172.16.10.9	CG	vlan1
+-----+-----+-----+-----+
```

```
Flags: C - Connected G - Gateway
```

```
RFController(config)#
```

```
RFController(config)#show ip route pc 2
```

```
+-----+-----+-----+-----+
| DESTINATION | GATEWAY | FLAGS | INTERFACE |
+-----+-----+-----+-----+
157.235.208.0/24	direct	C	vlan4
172.16.10.0/24	direct	C	vlan1
default	172.16.10.9	CG	vlan1
+-----+-----+-----+-----+Fl
```

```
ags: C - Connected G - Gateway
```

```
RFController(config)#
```

```
RFController(config)#show ip route vlan 1 on RFController
```

```
+-----+-----+-----+-----+
| DESTINATION | GATEWAY | FLAGS | INTERFACE |
+-----+-----+-----+-----+
| 172.16.10.0/24 | direct | C | vlan1 |
| default | 172.16.10.9 | CG | vlan1 |
+-----+-----+-----+-----+
```

```
Flags: C - Connected G - Gateway
```

```
RFController(config)#
```

```
RFController(config)#show ip route ge 1 on RFController
```

```
+-----+-----+-----+-----+
| DESTINATION | GATEWAY | FLAGS | INTERFACE |
+-----+-----+-----+-----+
172.16.12.0/24	direct	C	vlan3
172.16.11.0/24	direct	C	vlan2
172.16.10.0/24	direct	C	vlan1
+-----+-----+-----+-----+
```

```
Flags: C - Connected G - Gateway
```

```
RFController(config)#
```

```
RFController(config)#show ip routing on RFController
```

```
IP routing is enabled.
```

```
RFController(config)#
```

```
RFController(config)#show ip dhcp status on RFController
```

```
State of DHCP server: running
```

```
Interfaces: vlan2, vlan3
```

```
RFController(config)#
```

## ip-access-list-stats

### show commands

Displays IP access list statistics

---

#### NOTE

This command is not present in the USER EXEC Mode.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
show ip-access-list-stats {on <DEVICE-NAME>|<IP-ACCESS-LIST> {on
<DEVICE-NAME>}}
```

---

#### Parameters

- |                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{on &lt;DEVICE-NAME&gt; &lt;IP-ACCESS-L IST&gt; {on &lt;DEVICE-NAME&gt;}}</pre> | <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the Controller name</li> </ul> </li> <li>• &lt;IP-ACCESS-LIST&gt; – Specifies the name of the ip-access-list used to view statistics <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller name</li> </ul> </li> </ul> </li> </ul> |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

#### Example

```
RFController(config)#sh ip-access-list-stats
IP Access-list: # Restrict Management ACL #
  permit tcp any any eq ftp rule-precedence 1      Hitcount: 0
  permit tcp any any eq www rule-precedence 2      Hitcount: 41
  permit tcp any any eq ssh rule-precedence 3      Hitcount: 448
  permit tcp any any eq https rule-precedence 4      Hitcount: 0
  permit udp any any eq snmp rule-precedence 5      Hitcount: 0
  permit tcp any any eq telnet rule-precedence 6      Hitcount: 4
```

## licenses

### [show commands](#)

Displays installed licenses and usage information

---

**NOTE**

This command is not present in the 'Privileged Exec' mode.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
show licenses
```

**Parameters**

None

**Example**

```
RFController(config)#show licenses
Serial Number : 6268529900014

Device Licenses:
  AP-LICENSE
    String      :
8088bb045018988b85bc05750ab7dbc802885bcc680a96194dfbeedc28d4117058eb53bd8b
    Value       : 50
    Used        : 0
  AAP-LICENSE
    String      :
8088bb045018988b5985f7127ca1d354bc689885fcc6b625b695384946d4117058eb53bd8b
    Value       : 50
    Used        : 0
RFController(config)#
```

## lldp

### *show commands*

Displays Link Layer Discovery Protocol information on AP/Controller

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show lldp neighbors {on <DEVICE-NAME>}
```

### Parameters

---

neighbors {on <DEVICE-NAME>} Displays LLDP neighbor table information

- on <DEVICE-NAME> - On AP/Controller
- <DEVICE-NAME> - AP/Controller name

---

### Example

```
RFController(config)#show lldp neighbors
RFController(config)#

RFController(config)#show lldp neighbors on RFController
RFController(config)#
```



## logging

### show commands

Displays logging information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show logging {on <DEVICE-NAME>}
```

### Parameters

---

|                            |                                                     |
|----------------------------|-----------------------------------------------------|
| logging {on <DEVICE-NAME>} | Displays logging information on an AP or controller |
|----------------------------|-----------------------------------------------------|

---

### Example

```
RFController(config)#show logging ?
  on  On AP/Controller
  |   Output modifiers
  >   Output redirection
  >> Output redirection appending
  <cr>
```

```
RFController(config)#show logging on ?
  DEVICE-NAME  AP / Controller name
```

```
RFController(config)#show logging on RFController
```

```
Logging module: enabled
  Aggregation time: disabled
  Console logging: level warnings
  Monitor logging: disabled
  Buffered logging: level warnings
  Syslog logging: level warnings
  Facility: local7
```

```
Log Buffer (18226 bytes):
```

```
Jan 27 18:04:54 2010: %CERTMGR-4-CERT_EXPIRY: server certificate for
trustpoint mint_security_trustpoint has expired
Jan 27 18:04:54 2010: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint_security_trustpoint has expired
Jan 27 17:04:54 2010: %CERTMGR-4-CERT_EXPIRY: server certificate for
trustpoint mint_security_trustpoint has expired
Jan 27 17:04:54 2010: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint_security_trustpoint has expired
```

## 7 show commands

```
Jan 27 16:04:54 2010: %CERTMGR-4-CERT_EXPIRY: server certificate for
trustpoint mint_security_trustpoint has expired
Jan 27 16:04:54 2010: %CERTMGR-4-CERT_EXPIRY: ca certificate for trustpoint
mint.....
RFController(config)#
```

## mac-access-list-stats

### show commands

Displays MAC-access list statistics

---

#### NOTE

This command is not present in USER EXEC Mode.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
show mac-access-list-stats {on <DEVICE-NAME>|<IP-ACCESS-LIST> {on  
<DEVICE-NAME>}}
```

#### Parameters

---

- |                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {on <DEVICE-NAME> <br><MAC-ACCESS-LIST> {on<br><DEVICE-NAME>} | <ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller<ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; – Displays the AP/Controller name</li></ul></li><li>• &lt;MAC-ACCESS-LIST&gt; – Specifies the name of the MAC-access-list used to view statistics<ul style="list-style-type: none"><li>• on &lt;DEVICE-NAME&gt; – Displays information on the AP/Controller<ul style="list-style-type: none"><li>• &lt;DEVICE-NAME&gt; – Displays the AP/Controller name</li></ul></li></ul></li></ul> |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

#### Example

```
RFController(config)#show mac-access-list-stats on RFController  
RFController(config)#
```

## mac-address-table

### show commands

Displays MAC address table entries

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show mac-address-table {on <DEVICE-NAME>}
```

### Parameters

- 
- |                    |                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {on <DEVICE-NAME>} | <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - Displays information on the AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - Displays information on the AP/Controller name</li> </ul> |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

### Example

```
RFController(config)#show mac-address-table on RFController
```

| BRIDGE | VLAN | PORT | MAC               | FORWARD |
|--------|------|------|-------------------|---------|
| 1      | 1    | ge1  | 00-50-DA-EE-B5-5C | forward |
| 1      | 1    | ge1  | 00-A0-F8-00-00-00 | forward |
| 1      | 1    | ge1  | 00-02-B3-28-D1-55 | forward |
| 1      | 1    | ge1  | 00-A0-F8-68-D5-5D | forward |
| 1      | 1    | ge1  | 00-50-DA-95-11-13 | forward |
| 1      | 1    | ge1  | 00-15-70-38-06-53 | forward |
| 1      | 1    | ge1  | 00-15-70-41-9F-7F | forward |
| 1      | 1    | ge1  | 00-15-70-88-9E-C4 | forward |

```
RFController(config)#
```

## mint

### show commands

Displays MiNT protocol configuration commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show mint [dis|id|known-adopters|links|lsp|lsp-db|mlcp|neighbors
|route|security|stats]
show mint [dis {on <DEVICE-NAME>/links {detail on <DEVICE-NAME>/on
<DEVICE-NAME>}/lsp/lsp-db {detail on <DEVICE-NAME>/on <DEVICE-NAME>}/mlcp
{history on <DEVICE-NAME> /on <DEVICE-NAME>}/neighbors {details on
<DEVICE-NAME>/on <DEVICE-NAME>}/security pending-approvals]

show mint [detail|known-adopters|route|stats]{on <DEVICE-NAME>}
```

### Parameters

---

|                              |                                                                                  |
|------------------------------|----------------------------------------------------------------------------------|
| mint                         | • dis – Displays MiNT network DISes                                              |
| [dis id known-adopters links | • id – Displays the local MiNT ID                                                |
| detail  lsp                  | • known-adopters – Displays known possible, reachable adopters                   |
| lsp-db mlcp history          | • security pending-approvals – Displays MiNT security parameters                 |
| neighbors route              | • pending-approvals – Displays pending requests to join the MiNT security domain |
| security                     | • links detail – Displays MiNT networking links details                          |
| pending-approvals stats]     | • lsp – Displays the router's MiNT LSPs                                          |
|                              | • lsp-db details <AA.BB.CC.DD> – Displays MiNT LSP database details              |
|                              | • < AA.BB.CC.DD> – Specify the MiNT address in <AA.BB.CC.DD> format              |
|                              | • mlcp history – Displays MiNT link creation protocol status                     |
|                              | • neighbors detail – Displays adjacent MiNT peers details                        |
|                              | • route – Displays MiNT route table details                                      |
|                              | • stats – Displays MiNT related statistics                                       |
|                              | The following is common for the above:                                           |
|                              | • {on <DEVICE-NAME>} – On AP/Controller                                          |
|                              | • <DEVICE-NAME> – On AP/Controller name                                          |

---

## Example

```
RFController(config)#show mint stats
0 L1 neighbors
L1 LSP DB size 1 LSPs (0 KB)
1 L1 routes
Last SPF took 0s
SPF (re)calculated 1 times.
levels 1
base priority 180
dis priority 180
RFController(config)#
```

```
RFController(config)#show mint lsp
id 70.37.fa.be, level 1, seqnum 18640, 0 adjacencies, 0 extended-vlans,
expires in 1145 seconds, republish in 722 seconds, changed True,
ext-vlan FDB pri 0, 180 bytes
```

```
RFController(config)#show mint lsp-db
Level 1 LSPs
 70.37.fa.be: seqnum 18640, 0 adjacencies, 0 extended-vlans, expires in 1138
seconds
1 LSPs in level 1 database
```

```
RFController(config)#show mint route
Destination : Next-Hop(s)
70.37.fa.be : 70.37.FA.BE
00.00.00.00 : 00.00.00.00
RFController(config)#
```

```
RFController(config)#show mint known-adopters on RFController
70.37.FA.BE
RFController(config)#
```

## noc

### show commands

Displays NOC level information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show noc [client-list|device|domain [managers|statistics details]]
show noc device filter {offline|online|rf-domain [RF-DOMAIN|not RF-DOMAIN] }
```

### Parameters

---

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [client-list device domain<br>[managers statistics]] | <ul style="list-style-type: none"> <li>• client-list – Displays a list of clients at the NOC level</li> <li>• device filter {offline online rf-domain [RF-DOMAIN not RF-DOMAIN] – Displays device information for all devices in the network           <ul style="list-style-type: none"> <li>• filter {offline online rf-domain [RF-DOMAIN not RF-DOMAIN]} – Specifies the additional selection filter in getting table values               <ul style="list-style-type: none"> <li>• offline – Displays devices that are offline</li> <li>• online – Displays device that are online</li> <li>• rf-domain [RF-DOMAIN not RF-DOMAIN]– Displays devices on given RF Domain                   <ul style="list-style-type: none"> <li>• RF-DOMAIN – Specify RF Domain name</li> <li>• not – Inverts match selection</li> </ul> </li> </ul> </li> </ul> </li> <li>• domain [managers statistics] – Displays RF Domain wide information           <ul style="list-style-type: none"> <li>• managers – Displays list of RF Domain and managers</li> <li>• statistics details – Displays statistical information regarding RF Domain in detail</li> </ul> </li> </ul> |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config)#show noc device
+-----+-----+-----+-----+-----+-----+
|  MAC           |HOST-NAME   |  TYPE   |CLUSTER|RF-DOMAIN|ADOPTED-BY|ONOFF|
+-----+-----+-----+-----+-----+-----+
99-88-77-66-55-44	br7131-665544	br7131		default		offline
00-15-70-88-9E-C4	br7131-889EC4	br7131		default		offline
11-22-33-44-55-66	br650-445566	br650		default		offline
00-15-70-37-FA-BE	RFController	rfs7000		default		online
+-----+-----+-----+-----+-----+-----+
Total number of clients displayed: 4
RFController(config)#
```

```
RFController(config)#show noc domain statistics details
=====
=====
RF-Domain RFDOMAIN_UseCase1
Note: TX = AP->Client, RX = Client->AP
-----
-----
Data bytes           : ( TX + RX = Total ),  0 + 0 = 0 bytes
Data throughput      : ( TX + RX = Total ),  0 Kbps + 0 Kbps = 0 Kbps
Data packets         : ( TX + RX = Total ),  0 + 0 = 0 pkts
Data pkts/sec        : ( TX + RX = Total ),  0 + 0 = 0 pps
BCMC Packets         : ( TX + RX = Total ),  0 + 0 = 0 pkts
Management Packets   : ( TX + RX = Total ),  0 + 0 = 0 pkts
Packets Discarded    : 0 - Tx Dropped, 0 - Rx Errors
Indicators            : T = 0 @ Max user rate of 0 Kbps
Distribution          : 0 Clients, 0 radios
Client count Details : 0/0/0 (b/bg/bgn); 0/0 (a/an)
Stats Update Info    : 6 seconds - update interval, mode is auto
Threat Level         : 0
Cause of concern     :
Remedy                :
Last update           : 2010-01-31 10:30:22 by 00-15-70-37-FA-BE
-----
-----
Total number of RF-domain displayed: 1
RFController(config-rf-domain-RFDOMAIN_UseCase1)#
RFController(config)#
```

```
RFController(config)#show noc device filter online
-----
MAC      HOST-NAME      TYPE      CLUSTER      RF-DOMAIN      ADOPTED-BY
ONLINE
-----
00-15-70-37-FA-BE RFController rfs7000  RFDOMAI..echPubs      online
-----
Total number of clients displayed: 1
RFController(config)#
```

```
RFController(config)#show noc domain statistics details
=====RF-
Domain RFDOMAIN_TechPubs
Note: TX = AP->Client, RX = Client->AP
-----
-----
Data bytes           : ( TX + RX = Total ),  0 + 0 = 0 bytes
Data throughput      : ( TX + RX = Total ),  0 Kbps + 0 Kbps = 0 Kbps
```



```
Data packets           : ( TX + RX = Total ),  0 + 0 = 0 pkts
Data pkts/sec          : ( TX + RX = Total ),  0 + 0 = 0 pps
BCMC Packets           : ( TX + RX = Total ),  0 + 0 = 0 pkts
Management Packets    : ( TX + RX = Total ),  0 + 0 = 0 pkts
Packets Discarded     : 0 - Tx Dropped, 0 - Rx Errors
Indicators             : T = 0 @ Max user rate of 0 Kbps
Distribution           : 0 Clients, 0 radios
Client count Details   : 0/0/0 (b/bg/bgn); 0/0 (a/an)
Stats Update Info     : 6 seconds - update interval, mode is auto
Threat Level          : 1
Cause of concern       : no sensors enabled in RF-domain RFDOMAIN_TechPubs
Remedy                : enable AP detection
Last update           : 2011-01-09 08:44:15 by 00-15-70-37-FA-BE
-----
```

```
Total number of RF-domain displayed: 1
RFController(config)#
```

## ntp

### show commands

Displays *Network Time Protocol* (NTP) information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show ntp [associations {detail}|status] {on <DEVICE-NAME>}
```

### Parameters

---

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ntp [associations detail status]<br>{on <DEVICE-NAME>} | <p>Displays the <i>Network Time Protocol</i> (NTP) configuration</p> <ul style="list-style-type: none"> <li>• associations detail – Displays existing NTP associations             <ul style="list-style-type: none"> <li>• detail {on &lt;DEVICE-NAME&gt;} – Displays NTP association details</li> </ul> </li> <li>• status {on &lt;DEVICE-NAME&gt;} – Displays NTP status             <ul style="list-style-type: none"> <li>• on – On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; – On AP/Controller name</li> </ul> </li> </ul> |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController>show ntp associations
address      ref clock      st when poll reach delay offset disp
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
RFController>
```

```
RFController>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is
2**0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec
RFController>
```

```
RFController>show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is
2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFController>
```

## password-encryption

### [show commands](#)

Displays password encryption status information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show password-encryption status
```

### Parameters

---

|                            |                                                 |
|----------------------------|-------------------------------------------------|
| password-encryption status | Displays password encryption status information |
|----------------------------|-------------------------------------------------|

---

### Example

```
RFController(config)#show password-encryption status
Password encryption is disabled
RFController(config)#
```

## power

### show commands

Displays *power over ethernet* (PoE) information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
power [configuration|status] {on <DEVICE-NAME>}
```

### Parameters

[configuration|status] {on  
<DEVICE-NAME>}

- configuration – Displays the PoE configuration
- status – Displays the PoE status

The following are common for the above:

- on <DEVICE-NAME> – Displays information on the AP/Controller
- <DEVICE-NAME> – Displays information on the AP/Controller name

### Example

```
RFController(config)#show power status on RFController
System Voltage: 53.4 volts
Guard Band: 32 watts
Power Budget: 190 watts Power Consumption: 0 watts
poE device 1 temperature 35C
poE device 2 temperature 38C
```

```
-----
```

| PORT | VOLTS | mA | WATTS | CLASS | STATUS |
|------|-------|----|-------|-------|--------|
| ge1  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge2  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge3  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge4  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge5  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge6  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge7  | 0.0   | 0  | 0.0   | 0     | Off    |
| ge8  | 0.0   | 0  | 0.0   | 0     | Off    |

```
-----
```

```
RFController(config)#show power configuration
```

| PORT | PRIORITY | POWER LIMIT | ENABLED |
|------|----------|-------------|---------|
| ---  |          |             |         |
| ge1  | low      | 30.0W       | yes     |
| ge2  | low      | 30.0W       | yes     |
| ge3  | low      | 30.0W       | yes     |
| ge4  | low      | 30.0W       | yes     |
| ge5  | low      | 30.0W       | yes     |
| ge6  | low      | 30.0W       | yes     |
| ge7  | low      | 30.0W       | yes     |
| ge8  | low      | 30.0W       | yes     |
| ---  |          |             |         |
| ---  |          |             |         |

## remote-debug

### *show commands*

Displays remote debug session information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
show remote-debugging
```

### **Parameters**

None

### **Example**

```
RFController(config)#show remote-debug
live-pktcap
  Not running
wireless
  Not running
copy-crashinfo
  Not running
offline-pktcap
  Not running
copy-techsupport
  Not running
more
  Not running
RFController(config)#
```

## rf-domain-manager

### [show commands](#)

Displays RF Domain Manager selection details

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show rf-domain-manager
```

### Parameters

None

### Example

```
RFController(config)#show rf-domain-manager
RF Domain default
RF Domain Manager:
  ID: 70.37.fa.be
  Priority: 9
  Has IP connectivity
  Has non-mesh links
  Last change 12265 seconds ago
This device:
  Priority: 9
  Has IP connectivity
  Has non-mesh links
RFController(config)#
```

## role

### *show commands*

Displays role based firewall information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show role wireless-clients {on <DEVICE-OR-DOMAIN-NAME>}
```

### Parameters

---

|                                                  |                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wireless-clients {on<br><DEVICE-OR-DOMAIN-NAME>} | Mobile units associated with roles <ul style="list-style-type: none"><li>• on &lt;DEVICE-OR-DOMAIN NAME&gt; - Displays information on the AP/Controller or RF-Domain</li><li>• &lt;DEVICE-OR-DOMAIN NAME&gt; - Displays information on the AP/Controller/RF Domain name</li></ul> |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#show role wireless-clients on RFController
No ROLE statistics found.
RFController(config)#
```



## running-config

### show commands

Displays the contents of those configuration files where all configured MAC and IP access lists are applied to an interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show running-config {device/include-factory/interface/wlan}
show running-config device [DEVICE|self] {include-factory}
show running-config interface {<WORD>/ge<1-4>/include-factory/me1/pc/vlan}
show running-config interface {<WORD>/ge <1-4>/me1/port-channel <1-4>/vlan
<1-4094>} {include-factory}
show running-config wlan <WLAN> {include-factory}
```

### Parameters

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device [DEVICE self]<br>{include-factory}                                      | Displays device configuration <ul style="list-style-type: none"> <li>• DEVICE – Specifies a device MAC address to view detailed information</li> <li>• self – Displays the currently logged device <ul style="list-style-type: none"> <li>• include-factory – Includes factory defaults</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                              |
| include-factory                                                                | Includes default factory settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| interface {<WORD>/ge<br><1-4>/me1/pc <1-4>/vlan<br><1-4094>} {include-factory} | Displays configuration for configured interface <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specifies the interface name</li> <li>• ge &lt;1-4&gt; – Gigabit Ethernet interface from 1-4</li> <li>• include-factory – Includes factory defaults</li> <li>• me1 – Fast Ethernet interface</li> <li>• port-channel &lt;1-4&gt; – Port-Channel interface from 1-4</li> <li>• vlan &lt;1-4094&gt; – Specifies a VLAN index value from 1-4094</li> </ul> <p>The following parameter is common for all the above:</p> <ul style="list-style-type: none"> <li>• include-factory – Includes factory defaults</li> </ul> |
| wlan <WLAN><br>{include-factory}                                               | Displays configuration for a specific WLAN <ul style="list-style-type: none"> <li>• &lt;WLAN&gt; {include-factory} – Specifies the name of the WLAN</li> <li>• include-factory – Includes factory defaults</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                       |

### Example

```
RFController(config)#show running-config device self
!
firewall ratelimit-trust policy default
!
management-policy default
telnet
```

## 7 show commands

```
    http server
    ssh
    !
    firewall-policy default
    !
    mint-security-policy the_policy
    rejoin-timeout 35
    !
    device-discover-policy default
    !
    rfs7000 00-15-70-37-FA-BE
    hostname RFController
    no country-code
    bridge vlan 3
    bridge vlan 5
    ip arp trust
    ip dhcp trust
    ip igmp snooping querier version 2
    ip igmp snooping querier max-response-time 3
    ip igmp snooping querier timer expiry 89
    wep-shared-key-auth
    radius nas-identifier
    test.....
    ....
    RFController(config)

    RFController(config)#show running-config device 11-22-33-44-55-66
    include-factory
    !
    radio-qos-policy default
    wmm best-effort txop-limit 0
    wmm best-effort aifsn 3
    wmm best-effort cw-min 4
    wmm best-effort cw-max 6
    wmm background txop-limit 0
    wmm background aifsn 7
    wmm background cw-min 4
    wmm background cw-max 10
    wmm video txop-limit 94
    wmm video aifsn 1
    wmm video cw-min 3
    wmm video cw-max 4
    wmm voice txop-limit 47
    wmm voice aifsn 1
    wmm voice cw-min
    2.....
    RFController(config)#
```

## session-changes

### [show commands](#)

Displays the configuration changes made in this session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show session-changes
```

### Parameters

None

### Example

```
RFController(config)#show session-changes

No changes in this session

RFController(config)#
```

## session-config

### show commands

Displays the list of active open sessions on a device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show session-config {include-factory}
```

### Parameters

- 
- |                                  |                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------|
| session-config {include-factory} | Displays the contents of the current configuration                                              |
|                                  | <ul style="list-style-type: none"><li>• {include-factory} – Includes factory defaults</li></ul> |
- 

### Example

```
RFController(config)#show session-config
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
firewall-policy default
no ip dos tcp-sequence-past-window
!
igmp-snoop-policy default
no igmp-snooping
no querier
unknown-multicast-fwd
!
!
mint-policy global-default
!
wlan-qos-policy default
qos trust dscp
qos trust wmm
!
radio-qos-policy default
.....
.....
.....
.....
RFController(config)#
```

## sessions

### [show commands](#)

Displays CLI sessions

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show sessions {on <DEVICE-NAME>}
```

### Parameters

---

|                             |                                                  |
|-----------------------------|--------------------------------------------------|
| sessions {on <DEVICE-NAME>} | Displays CLI sessions on the device              |
| • on <DEVICE-NAME>          | - Displays information on the AP/Controller      |
| • <DEVICE- NAME>            | - Displays information on the AP/Controller name |

---

### Example

```
RFController(config)#show sessions
INDEX   COOKIE  NAME           START TIME           FROM
1       4       admin          Feb 16 13:05:36 2011 127.0.0.1
2       5       admin          Feb 16 13:06:19 2011 172.16.10.10
RFController(config)#
```

## smart-rf

### [show commands](#)

Displays Smart RF Management commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

show smart-rf [calibration-status|channel-distribution|history|
radio|interactive-calibration-config]
show smart-rf [calibration-status|channel-distribution|history|
interactive-calibration-config] {on <DOMAIN-NAME>}}
show smart-rf radio {<AA-BB-CC-DD-EE-FF>/activity/all-11an/
all-11bgn/energy/neighbors/on {<DOMAIN-NAME>}}
show smart-rf radio {AA-BB-CC-DD-EE-FF}/all-11an/all-11bgn} {on
<DOMAIN-NAME>}
show smart-rf radio energy {<AA-BB-CC-DD-EE-FF>/all-11an/all-11bgn} {on
<DOMAIN-NAME>}
show smart-rf radio neighbors {<AA-BB-CC-DD-EE-FF>/all-11an/all-11bgn} {on
<DOMAIN-NAME>}}]

```

## Parameters

|                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| calibration-status {on<br><DOMAIN-NAME>}                                                                             | <p>Displays smart-rf calibration status</p> <ul style="list-style-type: none"> <li>on &lt;DOMAIN NAME&gt; - Displays information on a RF Domain           <ul style="list-style-type: none"> <li>&lt;DOMAIN NAME&gt; - Displays information on a RF Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| channel-distribution {on<br><DOMAIN-NAME>}                                                                           | <p>Display smart-rf channel distribution</p> <ul style="list-style-type: none"> <li>on &lt;DOMAIN NAME&gt; - Displays information on a RF Domain           <ul style="list-style-type: none"> <li>&lt;DOMAIN NAME&gt; - Displays information on a RF Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| history {on<br><DOMAIN-NAME>}                                                                                        | <p>Displays smart-rf history</p> <ul style="list-style-type: none"> <li>on &lt;DOMAIN NAME&gt; - Displays information on a RF Domain           <ul style="list-style-type: none"> <li>&lt;DOMAIN NAME&gt; - Displays information on a RF Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| radio<br>{<AA-BB-CC-DD-EE-FF>  <br>activity   all-11an  <br>all-11bgn   energy  <br>neighbors   on<br><DOMAIN-NAME>} | <p>Displays radio related commands</p> <ul style="list-style-type: none"> <li>energy - All 11a radios currently in the configuration</li> <li>neighbors - All 11a radios currently in the configuration           <ul style="list-style-type: none"> <li>&lt;AA-BB-CC-DD-EE-FF&gt; - Radio MAC address in &lt;AA-BB-CC-DD-EE-FF&gt; format (for all radios)</li> </ul> </li> <li>activity - Displays number of power/channel /coverage hole related changes</li> <li>all-11an - All 11bg radios currently in the configuration</li> <li>all-11bgn - Displays radio energy</li> </ul> <p>The following are common for all the above:</p> <ul style="list-style-type: none"> <li>on &lt;DOMAIN NAME&gt; - Displays information on a RF Domain           <ul style="list-style-type: none"> <li>&lt;DOMAIN NAME&gt; - Displays information on a RF Domain name</li> </ul> </li> <li>on &lt;DOMAIN NAME&gt; - Displays information on a RF Domain</li> </ul> |
| interactive-calibration-config {on<br><DOMAIN-NAME>}                                                                 | <p>Displays simulated calibration configuration</p> <ul style="list-style-type: none"> <li>on &lt;DOMAIN NAME&gt; - Displays information on a RF Domain           <ul style="list-style-type: none"> <li>&lt;DOMAIN NAME&gt; - Displays information on a RF Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Example

```
RFController(config)#show smart-rf calibration-status
No calibration currently in progress
RFController(config)#

RFController(config)#show smart-rf history
RFController(config)#
```

## spanning-tree

### show commands

Displays spanning tree information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show spanning-tree mst {configuration/detail/instance/on}
show spanning-tree mst {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst configuration {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst detail {interface/on}
show spanning-tree mst detail interface
{<WORD>|ge<1-4>|me1|port-channel<1-4>|vlan <1-4094>} {on
<DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst detail {on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst instance <1-15> {interface/on}
show spanning-tree mst instance <1-15> interface <WORD>
{on <DEVICE-OR-DOMAIN-NAME>}
show spanning-tree mst instance {on <DEVICE-OR-DOMAIN-NAME>}
```



**Parameters**

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mst                                        | Displays Multiple Spanning Tree (MST) information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| configuration {on <DEVICE-OR-DOMAIN-NAME>} | <ul style="list-style-type: none"> <li>configuration – Displays configuration information</li> <li>{on &lt;DEVICE-OR-DOMAIN NAME&gt;} – Displays information on the AP/Controller <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN NAME&gt; – Displays information on the AP/Controller/RF-Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| detail {interface   on}                    | <p>Displays detailed information</p> <ul style="list-style-type: none"> <li>interface – Interface information <ul style="list-style-type: none"> <li>&lt;WORD&gt; – Interface name</li> <li>ge &lt;1-4&gt; – Gigabit Ethernet interface from 1-4</li> <li>me1 – Fast Ethernet interface</li> <li>port-channel &lt;1-4&gt; – Port Channel interface</li> <li>vlan &lt;1-4094&gt; – Select a value from 1 -4094 to set VLAN index</li> </ul> </li> </ul> <p>The following parameters are common for interface commands</p> <ul style="list-style-type: none"> <li>{on &lt;DEVICE-OR-DOMAIN NAME&gt;} – Displays information on the AP/Controller <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN NAME&gt; – Displays information on the AP/Controller/RF Domain name</li> </ul> </li> <li>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Displays information on the AP/Controller <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN NAME&gt; – Displays information on the AP/Controller/RF Domain name</li> </ul> </li> </ul> |
| instance <1-15> {interface   on}           | <p>Displays instance information</p> <ul style="list-style-type: none"> <li>&lt;1-15&gt; – Select an instance ID from 1-15</li> <li>interface &lt;WORD&gt; {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Interface information <ul style="list-style-type: none"> <li>&lt;WORD&gt; {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Specifies the interface name <ul style="list-style-type: none"> <li>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Displays information on the AP/Controller</li> <li>&lt;DEVICE-OR-DOMAIN NAME&gt; – Displays information on the AP/Controller/RF-Domain name</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| {on <DEVICE-OR-DOMAIN-NAME>}               | <ul style="list-style-type: none"> <li>{on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Displays information on the AP/Controller <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN NAME&gt; – Displays information on the AP/Controller/RF-Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Example**

```
RFController(config)#show spanning-tree mst configuration on RFController
%%
% MSTP Configuration Information for bridge 1 :
%%-----
% Format Id      : 0
% Name          : My Name
% Revision Level : 0
% Digest        : 0xac36177f50283cd4b83821d8ab26de62
%%-----

RFController(config)#

RFController(config)#show spanning-tree mst detail interface test on
RFController
% Bridge up - Spanning Tree Disabled
```

## 7 show commands

```
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

RFController(config)#

RFController(config)#show spanning-tree mst detail
% Bridge up - Spanning Tree Disabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max hops 20
% 1: CIST Root Id 800000157037fabf
% 1: CIST Reg Root Id 800000157037fabf
% 1: CIST Bridge Id 800000157037fabf
% portfast bpdu-filter disabled
% portfast bpdu-guard disabled
% portfast portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off

% ge4: Port 2004 - Id 87d4 - Role Disabled - State Forwarding
% ge4: Designated External Path Cost 0 - Internal Path Cost 0
% ge4: Configured Path Cost 11520 - Add type Implicit - ref count 1
% ge4: Designated Port Id 0 - CST Priority 128
% ge4: ge4: CIST Root 0000000000000000
% ge4: ge4: Regional Root 0000000000000000
% ge4: ge4: Designated Bridge 0000000000000000
% ge4: Message Age 0 - Max Age 0
% ge4: CIST Hello Time 0 - Forward Delay 0
% ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge4: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
% ge4: Portfast configured - Current portfast on
% ge4: portfast bpdu-guard enabled - Current portfast bpdu-guard off
% ge4: portfast bpdu-filter enabled - Current portfast bpdu-filter off
% ge4: no root guard configured - Current root guard off
% ge4: Configured Link Type point-to-point - Current point-to-point

% ge3: Port 2003 - Id 87d3 - Role Disabled - State Forwarding
% ge3: Designated External Path Cost 0 - Internal Path Cost 0
% ge3: Configured Path Cost 11520 - Add type Implicit - ref count 1
% ge3: Designated Port Id 0 - CST Priority
128.....
.....
RFController(config)#

RFController(config)#show spanning-tree mst instance 1 interface test on
RFController
RFController(config)#
```

## startup-config

### show commands

Displays the complete startup configuration script on the console

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show startup-config {include-factory}
```

### Parameters

---

|                                     |                                                                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| startup-config<br>{include-factory} | Displays the contents of the startup configuration <ul style="list-style-type: none"> <li>• include-factory – Includes factory defaults</li> </ul> |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config)#show startup-config include-factory
!
! Configuration of RFS7000 version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
  enable
  calibration wait-time 4
!
wlan-qos-policy default
!
wlan-qos-policy test
  voice-prioritization
  svp-prioritization
  wmm background cw-max 8
  wmm video txop-limit 9
  wmm voice cw-min 6
  wmm voice cw-max 6
  rate-limit client to-air max-burst-size 3
  rate-limit client to-air red-threshold video 101
  rate-limit client from-air rate 55
  rate-limit client from-air
red-.....
.....
RFController(config)#
```

## terminal

### [show commands](#)

Displays terminal configuration parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show terminal
```

### Parameters

None

### Example

```
RFController(config)#show terminal
Terminal Type: xterm
Length: 45      Width: 126
RFController(config)#
```

## timezone

### [show commands](#)

Displays the timezone of the AP or controller on the command prompt

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show timezone
```

### Parameters

---

|          |                       |
|----------|-----------------------|
| timezone | Displays the timezone |
|----------|-----------------------|

---

### Example

```
RFController(config)#show timezone  
Timezone is America/Los_Angeles
```

## upgrade-status

### show commands

Displays the status of the last image upgrade

---

#### NOTE

This command is not present in the USER EXEC Mode.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
show upgrade-status {detail {on <DEVICE-NAME>}|on <DEVICE-NAME>}
```

---

#### Parameters

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>upgrade-status {detail {on &lt;DEVICE-NAME&gt;} on &lt;DEVICE-NAME&gt;}</pre> | <p>Displays the last image-upgrade status</p> <ul style="list-style-type: none"> <li>• detail - Displays last image upgrade log <ul style="list-style-type: none"> <li>• on &lt;DEVICE-NAME&gt; - On AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - OnAP/Controller name</li> </ul> </li> </ul> </li> <li>• {on &lt;DEVICE-NAME&gt;} - On AP/Controller <ul style="list-style-type: none"> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> </ul> </li> </ul> |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

#### Example

```
RFController(config)#show upgrade-status detail on RFController
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 04:12:2011 08:44:00 UTC
-----
Running from partition /dev/mtdblock6, partition to update is /dev/mtdblock7
var2 is 6 percent full
/tmp is 6 percent full
Free Memory 155900 kB
FWU invoked via Linux shell
Validating image file header
Making file system
Extracting files (this can take some time).
Version of firmware update file is 5.1.0.0
Successful
RFController(config)#

RFController(config)#show upgrade-status on RFController
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : 04:12:20110 08:44:00 UTC
RFController(config)#
```

## version

### [show commands](#)

Displays a device's software and hardware version

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show version {on <DEVICE-NAME>}
```

### Parameters

---

|                           |                                                                                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| version {on <DEVICE-NAME> | Displays the software and hardware version on a device                                                                                                 |
|                           | <ul style="list-style-type: none"> <li>• {on &lt;DEVICE-NAME&gt;} - On AP/Controller</li> <li>• &lt;DEVICE-NAME&gt; - On AP/Controller name</li> </ul> |

---

### Example

```
RFController(config)#show version on RFController
RFS7000 version 5.1.0.0
Copyright (c) 2011 Brocade, Inc.
Booted from primary

RFS7000 uptime is 0 days, 04 hours 39 minutes
CPU is RMI XLR V0.4
255464 kB of on-board RAM
Base ethernet MAC address is 00-15-70-37-FA-BE
System serial number is 6268529900014
Model number is None
FPGA version is 3.41
RFController(config)#
```

## wireless

### show commands

Displays wireless configuration parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

show wireless [ap|client|domain|mesh| |radio|regulatory|sensor-server|
unsanctioned|wips|wlan]
show wireless ap {configured|detail|load-balancing|on}
show wireless ap detail {on <DEVICE-OR-DOMAIN-NAME>|<DEVICE-NAME> on
<DEVICE-OR-DOMAIN-NAME>}
show wireless ap load-balancing {on <DEVICE-NAME>}
show wireless ap on <DEVICE-OR-DOMAIN-NAME>
show wireless client {detail <AA-BB-CC-DD-EE-FF> on
<DEVICE-OR-DOMAIN-NAME>|filter|on <DEVICE-OR-DOMAIN-NAME> |statistics|tspec
<AA-BB-CC-DD-EE-FF>}
show wireless client filter [ip|state|wlan]
show wireless client statistics {detail <AA-BB-CC-DD-EE-FF>|on
<DEVICE-OR-DOMAIN-NAME>}|rf|traffic>window-data}
show wireless client statistics {rf|traffic} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless client window-data [<AA-BB-CC-DD-EE-FF> <1-2>|<WORD>]
show wireless client filter ip [<A.B.C.D>|not <A.B.C.D>]
show wireless client filter state [date-ready|not [data-ready|roaming]
|roaming]
show wireless client filter wlan [<WLAN>|not <WLAN>]
show wireless mesh links {on <DEVICE-OR-DOMAIN-NAME>}

show wireless radio {detail|on|statistics|tspec}
show wireless radio [detail|tspec] [<AA-BB-CC-DD-EE-FF><1-3>|<WORD>]
show wireless radio {on <DEVICE-OR-DOMAIN-NAME>}
show wireless radio statistics {detail|on|rf|traffic>window-data}
show wireless radio statistics { on <DEVICE-OR-DOMAIN-NAME> |rf {on
<DEVICE-OR-DOMAIN-NAME>}|traffic {on <DEVICE-OR-DOMAIN-NAME>}}
show wireless radio statistics {detail>window-data} {<AA-BB-CC-DD-EE-FF>
<1-3>|<WORD>}
show wireless regulatory [channel-info <WORD>|country-code <WORD>|
device-type]
show wireless regulatory device-type [br650|br7131|rfs4000] <WORD>
show wireless sensor-server {on <DEVICE-OR-DOMAIN-NAME>}
show wireless sanctioned aps {detail|statistics|on}
show wireless sanctioned aps {detail|statistics} {on <DEVICE-OR-DOMAIN-NAME>}
show wireless sanctioned aps {on <DEVICE-OR-DOMAIN-NAME>}

```



```

show wireless wips [event-history|client-blacklist]{on
<DEVICE-OR-DOMAIN-NAME>}
show wireless wlan {config|detail <WLAN>|on <DEVICE-OR-DOMAIN-NAME>|
policy-mappings|statistics|usage-mappings}
show wireless wlan statistics {<WLAN>|detail|on|traffic}
show wireless wlan statistics {<WLAN>|detail|traffic} {on
<DEVICE-OR-DOMAIN-NAME>}
show wireless wlan statistics {on <DEVICE-OR-DOMAIN-NAME>}

```

## Parameters

|                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap {configured detail<br> load-balancing on}                                                                             | <p>Displays information regarding managed access points</p> <ul style="list-style-type: none"> <li>configured – Displays information on all access points in configuration</li> <li>detail {on &lt;DEVICE-OR-DOMAIN-NAME&gt; &lt;DEVICE-NAME&gt; on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Displays detailed information for given AP <ul style="list-style-type: none"> <li>&lt;DEVICE-NAME&gt; – Specify AP MAC address or its hostname</li> </ul> </li> <li>load-balancing {on &lt;DEVICE-NAME&gt;} – Displays load balancing status on the specified device</li> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller or RF Domain <ul style="list-style-type: none"> <li>on – On AP/Controller or RF Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF Domain name</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| client {detail<br><AA-BB-CC-DD-EE-FF> filter on<br><DEVICE-OR-DOMAIN-NAME> <br> statistics tspec<br><AA-BB-CC-DD-EE-FF>} | <p>Displays information about clients</p> <ul style="list-style-type: none"> <li>detail &lt;AA-BB-CC-DD-EE-FF&gt; – Displays detailed information about a client <ul style="list-style-type: none"> <li>&lt;AA-BB-CC-DD-EE-FF&gt; – Specify the MAC address of the client</li> </ul> </li> <li>filter [ip state wlan] – Specifies an additional selection filter for getting table values <ul style="list-style-type: none"> <li>ip [&lt;A.B.C.D&gt; not] – Selection by IP address <ul style="list-style-type: none"> <li>&lt;A.B.C.D&gt; – Specifies the IP address</li> <li>not – Invert match selection</li> </ul> </li> <li>state [date-ready not [data-ready roaming]] roaming] – Selection based on state <ul style="list-style-type: none"> <li>date-ready – Clients in data-ready</li> <li>not [data-ready roaming] – Invert match selection</li> <li>roaming – Roaming clients</li> </ul> </li> <li>wlan – Displays clients on given WLAN <ul style="list-style-type: none"> <li>WLAN – Specifies the WLAN name</li> <li>not – Invert match selection</li> </ul> </li> </ul> </li> <li>on &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller or RF-Domain <ul style="list-style-type: none"> <li>&lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller or RF Domain name</li> </ul> </li> <li>statistics {detail &lt;AA-BB-CC-DD-EE-FF&gt; on &lt;DEVICE-OR-DOMAIN-NAME&gt; rf traffic window-data} – Displays statistical information for clients <ul style="list-style-type: none"> <li>detail &lt;AA-BB-CC-DD-EE-FF&gt; – Displays detailed information about a client <ul style="list-style-type: none"> <li>&lt;AA-BB-CC-DD-EE-FF&gt; – Enter the MAC address of a client</li> </ul> </li> <li>rf on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Displays information about RF related statistics</li> <li>traffic on &lt;DEVICE-OR-DOMAIN-NAME&gt; – Displays information about data traffic related statistics</li> </ul> </li> </ul> |

---

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• on &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller or RF-Domain             <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller or RF-Domain name</li> </ul> </li> <li>• window-data [ &lt;AA-BB-CC-DD-EE-FF&gt; &lt;1-2&gt; &lt;WORD&gt;] – Displays window statistics             <ul style="list-style-type: none"> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; &lt;1-2&gt; – Specifies the MAC address of the client                 <ul style="list-style-type: none"> <li>• &lt;1-2&gt; – Enter a numerical window number</li> <li>• &lt;WORD&gt; – Enter the client window-stats id in the form of MAC followed by window number: e.g. AA-BB-CC-DD-EE-FF:W1</li> </ul> </li> </ul> </li> <li>• tspec &lt;AA-BB-CC-DD-EE-FF&gt; – Displays detailed TSPEC information for clients             <ul style="list-style-type: none"> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; – Specifies the MAC address of the client</li> </ul> </li> <li>• wlan [WLAN not] – Displays client information for a given WLAN             <ul style="list-style-type: none"> <li>• &lt;WLAN&gt; – Specifies the WLAN name</li> <li>• not &lt;WLAN&gt; – Invert match selection                 <ul style="list-style-type: none"> <li>• &lt;WLAN&gt; – Specifies the WLAN name</li> </ul> </li> </ul> </li> </ul> | <hr/> <p>mesh links {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} Displays information on radio mesh</p> <ul style="list-style-type: none"> <li>• links – Displays information on the active links of the radio mesh             <ul style="list-style-type: none"> <li>• on – On AP/Controller or RF Domain                 <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF Domain name</li> </ul> </li> </ul> </li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| radio<br>{detail   on   statistics   tspec}                          | <p>Radio related commands. All parameters are optional.</p> <ul style="list-style-type: none"> <li>• on – On AP/Controller or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF-Domain name</li> </ul> </li> <li>• detail &lt;AA-BB-CC-DD-EE-FF&gt; &lt;1-3&gt;   &lt;WORD&gt; – Displays detailed information about a radio MAC</li> <li>• tspec &lt;AA-BB-CC-DD-EE-FF&gt; &lt;1-3&gt;   &lt;WORD&gt; – Displays detailed TSPEC information on a radio <ul style="list-style-type: none"> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; &lt;1-3&gt;   &lt;WORD&gt; – Specifies the MAC address of an AP <ul style="list-style-type: none"> <li>• &lt;1-3&gt; – Specifies the radio interface index between 1 and 3</li> <li>• &lt;WORD&gt; – Radio ID in the form AA-BB-CC-DD-EE-FF:RX</li> </ul> </li> </ul> </li> <li>• statistics {detail   on &lt;DEVICE-OR-DOMAIN-NAME&gt;   rf {on &lt;DEVICE-OR-DOMAIN-NAME&gt;}   traffic {on &lt;DEVICE-OR-DOMAIN-NAME&gt;   window-data}} – Displays statistics for all radios <ul style="list-style-type: none"> <li>• rf – Displays information about RF related statistics</li> <li>• traffic – Displays data traffic related statistics</li> </ul> </li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• on – On AP/Controller or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF Domain name</li> </ul> </li> <li>• on – On AP/Controller or RF-Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF-Domain name</li> </ul> </li> <li>• detail &lt;AA-BB-CC-DD-EE-FF&gt; &lt;1-3&gt;   &lt;WORD&gt; – Displays detailed statistical information about a radio</li> <li>• window-data – Displays Window stats (historical data over a time window) <ul style="list-style-type: none"> <li>• &lt;AA-BB-CC-DD-EE-FF &lt;1-3&gt; – Specifies a client MAC address</li> <li>• &lt;1-3&gt; – Specifies a radio interface index between 1 and 3</li> <li>• &lt;WORD&gt; – Specifies the radio window-stats id in the form of a MAC followed by the interface number and window number: For ex;. AA-BB-CC-DD-EE-FF:R1:W1</li> </ul> </li> </ul> |
| regulatory [channel-info <WORD>   country-code <WORD>   device-type] | <ul style="list-style-type: none"> <li>• channel-info &lt;WORD&gt; – Displays channel information</li> <li>• country-code – Displays the 2 letter ISO-3166 country code</li> <li>• device-type [br540   br7131   rfs4000] &lt;WORD&gt; – Displays device information based on the device type <ul style="list-style-type: none"> <li>• Mobility 650 Access Point &lt;WORD&gt; – Displays BR650 information</li> <li>• br7131 &lt;WORD&gt; – Displays BR7131 information</li> <li>• rfs4000 &lt;WORD&gt; – Displays the Mobility RFS4011 wireless controller model that houses radios</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| sensor-server {on <DEVICE-OR-DOMAIN-NAME>}                           | <p>Displays information about AirDefense sensor server configuration</p> <ul style="list-style-type: none"> <li>• on – On AP/controller or RF Domain <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

---

|                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>unsanctioned aps<br/>{detail statistics} {on<br/>&lt;DEVICE-OR-DOMAIN-NAME&gt;}</p>        | <p>Displays information about unauthorized APs Detected</p> <ul style="list-style-type: none"> <li>• aps – Lists detected unauthorized APs             <ul style="list-style-type: none"> <li>• detailed – Detailed information</li> <li>• statistics – Displays channel statistics</li> </ul> </li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• on – On AP/controller or RF-Domain             <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME – On AP/Controller/<br/>RF Domain name</li> </ul> </li> <li>• on – On AP/Controller or RF Domain             <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME – On AP/Controller/<br/>RF Domain name</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p>wips {event-history {on<br/>&lt;DEVICE-OR-DOMAIN-NAME&gt;<br/> client-blacklist</p>        | <p>Displays WIPS parameters</p> <ul style="list-style-type: none"> <li>• event-history {on &lt;DEVICE-OR-DOMAIN-NAME&gt;} – Displays an event history</li> <li>• client-blacklist – Displays details about blacklisted clients             <ul style="list-style-type: none"> <li>• on – On AP/Controller or RF Domain                 <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME – On AP/Controller/<br/>RF Domain name</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>wlan {config detail<br/>&lt;WLAN&gt; on <br/>policy-mapping statistics usage-mappings}</p> | <p>Displays wireless LAN parameters. The following information is displayed:</p> <ul style="list-style-type: none"> <li>• config – Displays the WLAN configuration</li> <li>• detail – Displays detailed configuration of specified WLAN configuration             <ul style="list-style-type: none"> <li>• WLAN – WLAN name</li> </ul> </li> <li>• policy-mappings – Displays the policy mappings for various WLANs</li> <li>• usage-mappings – Lists of all devices and profiles using the WLAN</li> <li>• statistics {WLAN detail on traffic} – Displays the WLAN statistics for:             <ul style="list-style-type: none"> <li>• WLAN – Displays WLAN for which the detailed statistics required</li> <li>• detail – Displays detailed statistics for all WLANs</li> <li>• on – On AP/Controller/RF-Domain                 <ul style="list-style-type: none"> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/<br/>RF Domain</li> </ul> </li> <li>• traffic – Displays data traffic related statistics</li> </ul> </li> <li>• The following parameters are common for the above:             <ul style="list-style-type: none"> <li>• on – On AP/Controller/RF Domain</li> <li>• &lt;DEVICE-OR-DOMAIN-NAME&gt; – On AP/Controller/RF Domain</li> </ul> </li> </ul> |

---

**Example**

```

RFController(config)#show wireless sensor server status on br7131-889EC4
RFController(config)#

RFController(config)#show wireless unauthorized aps detailed
Number of APs seen: 1
RFController(config)#
RFController(config)#show wireless wips mu-blacklist
No mobile units blacklisted
RFController(config)#

RFController(config)#show wireless wlan config
+-----+-----+-----+-----+-----+-----+
|  NAME  |  ENABLE  |  SSID  |  ENCRYPTION  |  AUTHENTICATION  |  VLAN  |
+-----+-----+-----+-----+-----+-----+
test	Y	test	none	none	1
brocade	Y	Brocade	none	none	1
wlan1	Y	wlan1	none	none	1
+-----+-----+-----+-----+-----+-----+

RFController(config)#

RFController(config)#show wireless wlan statistics
+-----+-----+-----+-----+-----+-----+-----+-----+
|WLAN|TX BYTES |RX BYTES|TX PKTS |RX PKTS |TX KBPS|RX KBPS |DROPPED |ERRORS |
+-----+-----+-----+-----+-----+-----+-----+-----+
|brocade | 0      | 0      | 0      | 0      | 0      | 0      | 0      | 0      |
|wlan1  | 0      | 0      | 0      | 0      | 0      | 0      | 0      | 0      |
+-----+-----+-----+-----+-----+-----+-----+-----+

Total number of wlan displayed: 2
RFController(config)#

RFController(config)#show wireless regulatory channel-info 1
Center frequency for channel 1 is 2412MHz
RFController(config)#

RFController(config)#show wireless regulatory country-code
ISO CODE                NAME
-----
al                       Algeria
ai                       Anguilla
ar                       Argentina
au                       Australia
at                       Austria
bs                       Bahamas
bh                       Bahrain
bb                       Barbados
by                       Belarus
be                       Belgium
bm                       Bermuda
bo                       Bolivia
bw                       Botswana
ba                       Bosnia-Herzegovina
br                       Brazil
bg                       Bulgaria
ca                       Canada
ky                       Cayman Islands
.....
RFController(config)#

```

## 7 show commands

```

RFController(config)#show wireless regulatory device-type br650 in
-----
# Channel Set Power(mW) Power (dBm) Placement DFS CAC(mins)
-----
1 1-13 4000 36 Indoor/Outdoor NA NA
2 36-64 200 23 Indoor Not Required 0
3 149-165 1000 30 Outdoor Not Required 0
4 149-165 200 23 Indoor Not Required 0
-----
RFController(config)#
RFController(config)#show wireless ap detail RFController on RFController

AP: 00-23-68-88-0D-A7
AP Name : RFController
Location : default
RF-Domain : default
Type : rfs4000
Model : RFS-4011-11110-US
Num of radios : 2
Num of clients : 0
Last Smart-RF time : not done
Stats update mode : auto
Stats interval : 6
Radio Modes :
    radio-1 : wlan
    radio-2 : wlan
Country-code : not-set
Site-Survivable : True
Last error :
Fault Detected : False
RFController(config)#
RFController(config)#show wireless ap load-balancing on default/RFController
AP: 00-23-68-88-0D-A7
Client requests on 5ghz : allowed
Client requests on 2.4ghz : allowed
Average AP load in neighborhood : 0 %
Load on this AP : 0 %
Total 2.4ghz band load in neighborhood : 0 %
Total 5ghz band load in neighborhood : 0 %
Configured band ratio 2.4ghz to 5ghz : 1:1
Current band ratio 2.4ghz to 5ghz : 0:0
Average 2.4ghz channel load in neighborhood : 0 %
Average 5ghz channel load in neighborhood : 0 %
Load on this AP's 2.4ghz channel : 0 %
Load on this AP's 5ghz channel : 0 %
Total number of APs displayed: 1
RFController(config)#
RFController(config)#show wireless ap on default
-----
MODE : radio modes - W = WLAN, S=Sensor, ' ' (Space) = radio not present
-----
AP-NAME AP-LOCATION RF-DOMAIN AP-MAC #RADIOS MODE #CLIENT LAST-CAL-TIME
-----
RFController default default 00-23-68-88-0D-A7 2 W-W 0 not done
-----
Total number of APs displayed: 1
RFController(config)#

```

## wwan

### show commands

Displays wireless WAN status

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller

### Syntax

```
show wwan [configuration|status] {on <DEVICE-OR-DOMAIN-NAME>}
```

### Parameters

---

|                                                          |                                                                   |
|----------------------------------------------------------|-------------------------------------------------------------------|
| wwan [configuration status] {on <DEVICE-OR-DOMAIN-NAME>} | • configuration – Displays wireless WAN configuration information |
|                                                          | • status – Displays wireless WAN status information               |
|                                                          | • on <DEVICE-OR-DOMAIN-NAME> – On AP/Controller or RF Domain      |
|                                                          | • <DEVICE-OR-DOMAIN-NAME> – On AP / Controller/RF Domain name     |

---

### Example

```
RFController(config-device-00-23-68-88-0D-A7)*#show wwan configuration on
RFController
>>> WWAN Configuration:
+-----+
| Access Point Name : isp.cingular
| User Name       : testuser
| Cryptomap      : map1
+-----+
RFController(config-device-00-23-68-88-0D-A7)#

RFController(config-device-00-23-68-88-0D-A7)#show wwan status on RFController
>>> WWAN Status:
+-----+
| State : ACTIVE
| DNS1  : 209.183.54.151
| DNS2  : 209.183.54.151
+-----+
RFController(config-device-00-23-68-88-0D-A7)#
```

## 7 show commands



# Profiles

---

## In this chapter

- [Creating profiles](#) ..... 408
- [Device specific commands](#) ..... 524

Profiles enable administrators to assign a common set of configuration parameters and policies to controllers and Access Points. Profiles can be used to assign common or unique network, wireless and security parameters to Wireless Controllers and Access Points across a large, multi segment site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The controller supports both default and user defined profiles implementing new features or updating existing parameters to groups of Wireless Controllers or Access Points. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

The system maintains a couple of default profiles. The default profile is applied to the wireless controller automatically, and default AP profiles are applied to the APs that are automatically discovered by the wireless controller. After adoption, if a change is made in one of the parameters in the profile, that change is reflected across all the APs using the same profile.

User defined profiles are manually created for each supported Wireless Controller and Access Point model. User defined profiles can be manually assigned or automatically assigned to Access Points.

- BR650 – Adds a Mobility 650 Access Point profile
- BR7131 – Adds a Mobility 7131 Series Access Point profile
- RFS4000 – Adds a Brocade Mobility RFS4000 wireless controller profile
- RFS6000 – Adds a Brocade Mobility RFS6000 wireless controller profile
- RFS7000 – Adds a Brocade Mobility RFS7000 wireless controller profile

Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

```
RFController(config)#profile rfs7000 default-rfs7000
RFController(config-profile-default-rfs7000)#
```

```
RFController(config)#profile br7131 default-br7131
RFController(config-profile-default-br7131)#
```

---

### NOTE

The commands present under 'Profiles' are also available under the 'Device mode'. The additional commands specific to the 'Device mode' are listed separately. Refer to ["device mode commands"](#) on page 524 for more information.

---

## Creating profiles

Table 16 Summarizes Profile Commands

**TABLE 16** profile commands

| Command                                        | Description                                                          | Reference                |
|------------------------------------------------|----------------------------------------------------------------------|--------------------------|
| <a href="#">aaa</a>                            | Configures AAA settings                                              | <a href="#">page 410</a> |
| <a href="#">ap-upgrade</a>                     | Enables an automatic adopted AP firmware upgrade                     | <a href="#">page 416</a> |
| <a href="#">arp</a>                            | Configures the static address resolution protocol                    | <a href="#">page 412</a> |
| <a href="#">auto-learn-staging-config</a>      | Enables network configuration learning of the devices                | <a href="#">page 414</a> |
| <a href="#">autoinstall</a>                    | Configures auto install feature                                      | <a href="#">page 415</a> |
| <a href="#">bridge</a>                         | Configures bridge specific commands                                  | <a href="#">page 418</a> |
| <a href="#">cdp</a>                            | Performs the <i>Cisco Discovery Protocol</i> (CDP) on a device       | <a href="#">page 428</a> |
| <a href="#">cluster</a>                        | Defines the cluster-name                                             | <a href="#">page 429</a> |
| <a href="#">configuration-persistence</a>      | Enables persistence of configuration across reloads                  | <a href="#">page 431</a> |
| <a href="#">controller</a>                     | Configures a WLAN controller                                         | <a href="#">page 432</a> |
| <a href="#">crypto</a>                         | Configures crypto settings                                           | <a href="#">page 434</a> |
| <a href="#">dscp-mapping</a>                   | Configures an IP DSCP to 802.1p priority mapping for untagged frames | <a href="#">page 448</a> |
| <a href="#">email-notification</a>             | Configures email notification                                        | <a href="#">page 450</a> |
| <a href="#">enforce-version</a>                | Checks the firmware versions of devices before interoperating        | <a href="#">page 452</a> |
| <a href="#">events</a>                         | Displays system event messages                                       | <a href="#">page 454</a> |
| <a href="#">ip</a>                             | Configures a selected Internet Protocol component                    | <a href="#">page 455</a> |
| <a href="#">interface</a>                      | Selects an interface to configure                                    | <a href="#">page 462</a> |
| <a href="#">led</a>                            | Turns device LEDs on/off                                             | <a href="#">page 492</a> |
| <a href="#">legacy-auto-downgrade</a>          | Enables a legacy device firmware auto downgrade                      | <a href="#">page 492</a> |
| <a href="#">legacy-auto-update</a>             | Enables a legacy device firmware auto update                         | <a href="#">page 494</a> |
| <a href="#">lldp</a>                           | Configures <i>Link Layer Discovery Protocol</i> (lldp)               | <a href="#">page 495</a> |
| <a href="#">load-balancing</a>                 | Configures load balancing parameters                                 | <a href="#">page 496</a> |
| <a href="#">local</a>                          | Creates a local user authentication database for VPN                 | <a href="#">page 498</a> |
| <a href="#">logging</a>                        | Modifies message logging facilities                                  | <a href="#">page 499</a> |
| <a href="#">mac-address-table</a>              | Configures the MAC address table                                     | <a href="#">page 501</a> |
| <a href="#">mint</a>                           | Configures the MiNT protocol                                         | <a href="#">page 502</a> |
| <a href="#">misconfiguration-recovery-time</a> | Verifies controller connectivity after the configuration is received | <a href="#">page 505</a> |
| <a href="#">monitor</a>                        | Enables critical resource monitoring                                 | <a href="#">page 506</a> |

**TABLE 16** profile commands

| <b>Command</b>                     | <b>Description</b>                                             | <b>Reference</b>         |
|------------------------------------|----------------------------------------------------------------|--------------------------|
| <i>neighbor-inactivity-timeout</i> | Configures neighbor inactivity timeout factor                  | <a href="#">page 507</a> |
| <i>neighbor-info-interval</i>      | Configures neighbor information exchange interval              | <a href="#">page 508</a> |
| <i>no</i>                          | Negates a command or sets its default values                   | <a href="#">page 509</a> |
| <i>noc</i>                         | Configures the noc related settings                            | <a href="#">page 510</a> |
| <i>ntp</i>                         | Configures an NTP server                                       | <a href="#">page 511</a> |
| <i>preferred-controller-group</i>  | Specifies the controller group the system prefers for adoption | <a href="#">page 512</a> |
| <i>power-config</i>                | Configures the power mode feature                              | <a href="#">page 513</a> |
| <i>radius</i>                      | Configures device level radius authentication parameters       | <a href="#">page 514</a> |
| <i>rf-domain-manager</i>           | Enables the rf-domain-manager feature                          | <a href="#">page 515</a> |
| <i>service</i>                     | Sets service commands                                          | <a href="#">page 516</a> |
| <i>spanning-tree</i>               | Configures spanning tree commands                              | <a href="#">page 517</a> |
| <i>use</i>                         | Defines the settings used by this feature                      | <a href="#">page 520</a> |
| <i>vpn</i>                         | Configures VPN settings                                        | <a href="#">page 522</a> |
| <i>wep-shared-key-auth</i>         | Enables support for 802.11 WEP shared key authentication       | <a href="#">page 523</a> |

## aaa

### *profile commands*

Configures VPN AAA authentication settings on the device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

aaa vpn-authentication
aaa vpn-authentication [primary|secondary] <A.B.C.D> key [0 <WORD>|2
<WORD>|<WORD>] {auth-port <1024-65535>}

```

### Parameters

---

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vpn-authentication            | Configures RADIUS settings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| [primary secondary] <A.B.C.D> | <ul style="list-style-type: none"> <li>• primary – Sets primary RADIUS server settings</li> <li>• secondary – Sets secondary RADIUS server settings</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| key [0 <WORD> 2               | The following parameters are common for the above:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <WORD> <WORD> ]               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| {auth-port <1024-65535>}      | <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Specifies the IP address for the RADIUS server</li> <li>• key [0 2 &lt;WORD&gt;] – Sets the RADIUS client preshared key; this key should match the RADIUS server <ul style="list-style-type: none"> <li>• 0 – Enter a clear text secret</li> <li>• 2 – Enter an encrypted secret</li> <li>• &lt;WORD&gt; – Specifies the shared secret up to 32 characters</li> </ul> </li> <li>• {auth-port &lt;1024-65535&gt;} – Sets the RADIUS server authentication port. Enter a port value between 1024 and 65535.</li> </ul> |

---

### Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server.

### Example

```

RFController(config-profile-default-rfs7000)#aaa vpn-authentication secondary
172.16.10.8 key symbol231 authport 1025
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
aaa vpn-authentication secondary 1.2.3.4 key 0 brocade123 authport 1025
interface me1
interface ge1

```

```
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
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
use firewall-policy default
service pm sys-restart
RFController(config-profile-default-rfs7000)#
```

## arp

### *profile commands*

Configures the address resolution protocol parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
arp [<IP>|timeout
arp <IP> <MAC> arpa [<L3-INTERFACE-NAME>|vlan <VLAN>] {[dhcp-server/router]}
arp timeout <TIME>
```

### Parameters

|                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>&lt;IP&gt; &lt;MAC&gt; arpa [&lt;L3-INTERFACE-NAME&gt;   vlan &lt;VLAN&gt;] {[dhcp-server/router] }</pre> | <p>Configures a static ARP entry for a given IPv4 IP address.</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – The static IP address to configure the ARP entry for</li> <li>• &lt;MAC&gt; – The MAC address to be associated with the IP and SVI</li> <li>• arpa – The type of ARP. <ul style="list-style-type: none"> <li>• &lt;L3-INTERFACE-NAME&gt; – Sets the router interface name</li> <li>• vlan &lt;VLAN&gt; – Sets a switch vlan interface where &lt;VLAN&gt; is the SVI interface name. <ul style="list-style-type: none"> <li>• dhcp-server – Optional. Sets the ARP entry for a dhcp-server</li> <li>• router – Optional. Sets the ARP entry for a router.</li> </ul> </li> </ul> </li> </ul> |
| <pre>timeout &lt;TIME&gt;</pre>                                                                                | <p>Sets the ARP timeout value.</p> <ul style="list-style-type: none"> <li>• &lt;TIME&gt; – Sets the ARP entry timeout value in seconds. Enter a value in the range 15-86400 seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

### Example

```
RFController(config-profile-default-rfs7000)#arp timeout 2000
RFControllerconfig-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  arp timeout 2000
  no autoinstall configuration
  no autoinstall firmware
  crypto isakmp policy default
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  interface me1
  interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
RFController(config-profile-default-rfs7000)#arp 172.16.10.10
45-bc-22-38-16-3F arpa vlan 3 dhcp-server
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
```

```
arp 172.16.10.10 45-bc-22-38-16-3F arpa vlan3 dhcp-server
arp timeout 2000
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
```

### auto-learn-staging-config

#### *profile commands*

Enables network configuration learning of the devices which come for adoption automatically

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
auto-learn-staging-config
```

#### **Parameters**

None

#### **Example**

```
RFController(config-profile-default-rfs7000)#auto-learn-staging-config
```



## autoinstall

### *profile commands*

Auto installs the controller image

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
autoinstall [configuration|firmware]
```

### Parameters

|               |                                                       |
|---------------|-------------------------------------------------------|
| configuration | Installs configuration setup parameters automatically |
| firmware      | Installs firmware image automatically                 |

### Example

```
RFController(config-profile-default-rfs7000)#autoinstall configuration

RFController(config-profile-default-rfs7000)#autoinstall firmware version
5.1.0.0
```

## ap-upgrade

### *profile commands*

Enables an automatic firmware upgrade for an adopted AP

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ap-upgrade [auto|count <1-20>]
```

### Parameters

|              |                                                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto         | Enables automatic adopted AP firmware upgrade                                                                                                                    |
| count <1-20> | Sets the concurrent upgrade limit <ul style="list-style-type: none"><li>• &lt;1-20&gt; - Enter the number of concurrent upgrades that can be performed</li></ul> |

### Example

```
RFController(config-profile-default-rfs7000)#ap-upgrade count 7
```

## bridge commands

### [profile commands](#)

Configures the Ethernet Bridging commands.

| Command                | Description                                 | Reference                |
|------------------------|---------------------------------------------|--------------------------|
| <a href="#">bridge</a> | Configures the Ethernet Bridging parameters | <a href="#">page 418</a> |

## bridge

### *profile commands*

Configures bridge specific commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

---

### NOTE

The interfaces mentioned below are supported as follows:

ge <index> – Mobility RFS7000 and Mobility RFS4000 support 4 GEs, Mobility RFS6000 supports 8 GEs

me1 – Only supported on Mobility RFS7000 and Mobility RFS6000 Controllers

---

### Syntax

```
bridge vlan <1-4095>
```

### Parameters

---

|               |                                             |
|---------------|---------------------------------------------|
| vlan <1-4095> | Enter a VLAN index value between 1 and 4095 |
|---------------|---------------------------------------------|

---

### Usage Guidelines

Creating customized filter schemes for bridged networks limits the amount of unnecessary traffic processed and distributed by the bridging equipment.

If a bridge does not hear *bridge protocol data units* (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, assume the network has changed and recomputed the spanning-tree topology.

### Example

```
RFController(config-profile-default-rfs7000)#bridge vlan 5
RFController(config-profile-default-rfs7000)#
```

## bridge-vlan mode commands

Table 17 Summarizes bridge-vlan-mode commands

**TABLE 17** bridge-vlan mode commands

| Command                              | Description                                                 | Reference                |
|--------------------------------------|-------------------------------------------------------------|--------------------------|
| <i>description</i>                   | Defines the VLAN description                                | <a href="#">page 421</a> |
| <i>edge-vlan</i>                     | Enables edge VLAN mode                                      | <a href="#">page 422</a> |
| <i>ip</i>                            | Configures the selected Internet Protocol (IP) component    | <a href="#">page 423</a> |
| <i>no</i>                            | Negates a command or sets its default values                | <a href="#">page 425</a> |
| <i>stateful-packet-inspection-12</i> | Enables a stateful packet inspection in the layer2 firewall | <a href="#">page 426</a> |

## *bridging-mode*

### *bridge-vlan mode commands*

Configures how the packets on the selected VLAN are bridged.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
bridging-mode [auto|isolated-tunnel|local|tunnel]
```

### **Parameters**

---

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto isolated-tunnel local tunnel | <ul style="list-style-type: none"> <li>• auto – Choose bridging mode automatically to match WLAN, vlan, and bridging-mode configuration</li> <li>• isolated-tunnel – Bridge packets between local ethernet ports and any local radios, and pass tunneled packets through without detunneling them</li> <li>• local – Bridge packets normally, between the local ethernet ports and local radios (if any)</li> <li>• tunnel – Bridge packets between local ethernet ports, any local radios, and tunnels to other APs and wireless-switches</li> </ul> |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-profile default-rfs7000-bridge-vlan-1)#bridging-mode
isolated-tunnel
RFController(config-profile default-rfs7000-bridge-vlan-1)#show context
bridge vlan 1
  bridging-mode isolated-tunnel
  ip igmp snooping
  ip igmp snooping querier
RFController(config-profile default-rfs7000-bridge-vlan-1)#
```

## *description*

### *bridge-vlan mode commands*

Sets a description of a Bridged VLAN.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
description <WORD>
```

### **Parameters**

---

|                    |                              |
|--------------------|------------------------------|
| description <WORD> | Defines the VLAN description |
|--------------------|------------------------------|

---

### **Example**

```
RFController(config-profile default-rfs7000-bridge-vlan-1)#description "This
is a description for the bridged VLAN"
RFController(config-profile default-rfs7000-bridge-vlan-1)#show context
bridge vlan 1
description This\ is\ a\ description\ for\ the\ bridged\ VLAN
bridging-mode isolated-tunnel
ip igmp snooping
ip igmp snooping querier
```

### *edge-vlan*

#### *bridge-vlan mode commands*

Enables the edge VLAN mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
edge-vlan
```

#### **Parameters**

None

#### **Example**

```
RFController(config-profile default-rfs7000-bridge-vlan-5)#edge-vlan  
RFController(config-profile default-rfs7000-bridge-vlan-5)#
```



## *ip*

### *bridge-vlan mode commands*

Configures the selected Internet Protocol (IP) component

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
ip [arp trust|dhcp trust|igmp]
ip igmp snooping {mrouter/querier/unknown-multicast}
ip igmp snooping mrouter [interface <WORD>|learn pim-dvrp]
ip igmp snooping querier {address <A.B.C.D>/max-response-time <1-25>/timer
expiry <60-300>/version <1-3>}
```

**Parameters**

|                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| arp trust                                                                                                                                                  | Configures an ARP component <ul style="list-style-type: none"> <li>trust – Trust ARP responses on VLAN</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| dhcp trust                                                                                                                                                 | Configures DHCP components <ul style="list-style-type: none"> <li>trust – Trust DHCP responses on a VLAN</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| igmp snooping {mrouter(interface <WORD> learn querier {address <A.B.C.D> max-response-time <1-25> timer expiry <60-300> version <1-3>}) unknown-multicast} | Configures <i>Internet Group Management Protocol</i> (IGMP) <ul style="list-style-type: none"> <li>snooping {mrouter querier unknown-multicast} – Configures IGMP snooping <ul style="list-style-type: none"> <li>mrouter [interface &lt;WORD&gt; learn pim-dvrrp] – Configures a multicast router <ul style="list-style-type: none"> <li>interface &lt;WORD&gt; – Specifies the interfaces to be configured</li> <li>learn pim-dvrrp – Sets the multicast router learning protocol <ul style="list-style-type: none"> <li>pim-dvrrp – Learns mrouter through PIM or DVRP protocols.</li> </ul> </li> </ul> </li> <li>querier {address &lt;A.B.C.D&gt; max-response-time &lt;1-25&gt; timer expiry&lt;60-300&gt; version &lt;1-3&gt;} – Configures IGMP querier <ul style="list-style-type: none"> <li>address &lt;A.B.C.D&gt; – Configures an IGMP querier source IP address <ul style="list-style-type: none"> <li>&lt;A.B&gt;C.D&gt; – Specifies an IGMP querier source IP address</li> </ul> </li> <li>max-response-time &lt;1-25&gt; – Configures an IGMP querier maximum response time (sec) <ul style="list-style-type: none"> <li>&lt;1-25&gt; – Specifies an IGMP querier maximum response time (sec)</li> </ul> </li> <li>timer expiry &lt;60-300&gt; – Configures the IGMP querier timer <ul style="list-style-type: none"> <li>expiry &lt;60-3000&gt; – Specifies an IGMP querier other querier time out (sec)</li> </ul> </li> <li>version &lt;1-3&gt; – Configures an IGMP version <ul style="list-style-type: none"> <li>&lt;1-3&gt; – Specifies the IGMP the version</li> </ul> </li> </ul> </li> <li>unknown-multicast – Forwards unknown multicast packets</li> </ul> </li></ul> |

**Example**

```

RFController(config-profile default-rfs7000-bridge-vlan-5)#ip arp trust
RFController(config-profile default-rfs7000-bridge-vlan-5)#

RFController(config-profile default-rfs7000-bridge-vlan-5)#ip dhcp trust
RFController(config-profile default-rfs7000-bridge-vlan-5)#

RFController(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping
mrouter learn pim-dvrrp
RFController(config-profile default-rfs7000-bridge-vlan-5)#
RFController(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping
mrouter interface gel
RFController(config-profile default-rfs7000-bridge-vlan-5)#
RFController(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping
querier max-response-time 5
RFController(config-profile default-rfs7000-bridge-vlan-5)#
RFController(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping
querier version 2
RFController(config-profile default-rfs7000-bridge-vlan-5)#
RFController(config-profile default-rfs7000-bridge-vlan-5)#ip igmp snooping
querier timer expiry 89
RFController(config-profile default-rfs7000-bridge-vlan-5)#

```

**no****bridge-vlan mode commands**

Negates a command or set its defaults

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [description|edge-vlan|extended-vlan|ip|overlaid-vlan|
stateful-packet-inspection-l2|use]
```

**Parameters**

|                               |                                                          |
|-------------------------------|----------------------------------------------------------|
| description                   | Removes VLAN description                                 |
| edge-vlan                     | Enables edge VLAN mode                                   |
| extended-vlan                 | Enables extended VLAN mode                               |
| ip                            | Configures the selected Internet Protocol (IP) component |
| overlaid-vlan                 | Disables overlaid VLAN mode                              |
| stateful-packet-inspection-l2 | Disables stateful packet inspection in layer2 firewall   |
| use                           | Uses preconfigured access lists with this bridge policy  |

**Example**

```
RFController(config-profile default-rfs7000-bridge-vlan-5)#no description
RFController(config-profile default-rfs7000-bridge-vlan-5)#

RFController(config-profile default-rfs7000-bridge-vlan-5)#no ip igmp snooping
mrouter interface gel
RFController(config-profile default-rfs7000-bridge-vlan-5)#

RFController(config-profile default-rfs7000-bridge-vlan-5)#no ip igmp snooping
mrouter learn pim-dvmrp
RFController(config-profile default-rfs7000-bridge-vlan-5)#

RFController(config-profile default-rfs7000-bridge-vlan-5)#no ip igmp snooping
querier max-response-time
RFController(config-profile default-rfs7000-bridge-vlan-5)#

RFController(config-profile default-rfs7000-bridge-vlan-5)#no ip igmp
querier version
RFController(config-profile default-rfs7000-bridge-vlan-5)#
```

### *stateful-packet-inspection-12*

#### *bridge-vlan mode commands*

Enables a stateful packet inspection at a layer2 firewall

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
stateful-packet-inspection-12
```

#### **Parameters**

None

#### **Example**

```
RFController(config-profile  
defalut-rfs7000-bridge-vlan-2)#stateful-packet-inspection-12  
RFController(config-profile defalut-rfs7000-bridge-vlan-2)#
```

**Use****bridge-vlan mode commands**

Uses preconfigured access lists with this bridge policy. Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
use [ip-access-list|mac-access-list]
use ip-access-list ext-vlan out <IP-ACCESS-LIST>
use mac-access-list ext-vlan out <MAC-ACCESS-LIST>
```

**Parameters**


---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list mac-access-list] | <ul style="list-style-type: none"> <li>• ip-access-list – Uses IP access list</li> <li>• mac-access-list – Uses MAC access list           <ul style="list-style-type: none"> <li>• ext-vlan – Enables extended-VLAN on the selected access list               <ul style="list-style-type: none"> <li>• out – Applies ACL on the outgoing packets</li> <li>• &lt;IP-ACCESS_LIST&gt; &lt;MAC-ACCESS-LIST&gt; – Specify the access list name as IP ACL or MAC ACL</li> </ul> </li> </ul> </li> </ul> |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-profile default-rfs7000-bridge-vlan-1)#use ip-access-list
ext-vlan out test
RFController(config-profile default-rfs7000-bridge-vlan-1)#
```

**NOTE**

The commands write, clrscr, help, exit, end, commit, do revert, service, and show are common for all the commands. For more information, see [Chapter 6, Common Commands](#).

---

## cdp

### *profile commands*

Operates the *Cisco Discovery Protocol* (CDP) on the device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
cdp [holdtime <10-1800>|run|timer <5-900>]
```

### Parameters

|                    |                                                                                     |
|--------------------|-------------------------------------------------------------------------------------|
| holdtime <10-1800> | Specifies the holdtime value transmitted in CDP packets between 10 and 1800 seconds |
| run                | Enables CDP sniffing and transmit globally                                          |
| timer <5-900>      | Specifies the timer value between 5 and 900 seconds                                 |

### Example

```
RFController(config-profile-default-rfs7000)#cdp run
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default)#cdp holdtime 11
RFController(config-profile-default)#

RFController(config-profile-default)#cdp timer 15
RFController(config-profile-default)#
```

## cluster

### *profile commands*

Sets the cluster configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
cluster [auto-revert|auto-revert-delay|handle-stp|member|mode|name]
cluster member [ip <A.B.C.D>|vlan <1-4094>]
cluster mode [active|standby]
cluster name <WORD>]
```

### Parameters

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto-revert                            | Enables auto-revert                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| auto-revert-delay<br><1-1800>          | Configures auto-revert-delay between 1 and 1800 minutes                                                                                                                                                                                                                                                                                                                                                                                                                                |
| handle-stp                             | Configures STP convergence                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| member [ip <A.B.C.D> vlan<br><1-4094>] | Adds a cluster member <ul style="list-style-type: none"> <li>• ip &lt;A.B.C.D&gt; - Sets the IP address of the cluster member               <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; - Specifies the IP address to configure</li> </ul> </li> <li>• vlan &lt;1-4094&gt; - Sets the VLAN on which cluster members are reachable               <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specifies the VLAN index between 1- 4094</li> </ul> </li> </ul> |
| mode [active standby]                  | Configures the cluster mode as either active or standby <ul style="list-style-type: none"> <li>• active - Active mode</li> <li>• standby - Standby mode</li> </ul>                                                                                                                                                                                                                                                                                                                     |
| name <WORD>                            | Configures cluster name                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

### Example

```
RFController(config-profile-default-rfs7000)#cluster name cluster1
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#cluster member ip 172.16.10.3
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#cluster mode active
RFController(config-profile-default-rfs7000)#
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  bridge vlan 1
  description Vlan1
  .....
```

## 8 Creating profiles

```
cluster name cluster1  
cluster member ip 172.16.10.3  
cluster member vlan 1
```

```
RFController(config-profile-default-rfs7000)#cluster auto-revert-delay 10  
RFController(config-profile-default-rfs7000)#
```



## configuration-persistence

### *profile commands*

Enables persistence of configuration across reloads

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
configuration-persistence {secure}
```

### Parameters

---

|        |                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------|
| secure | Optional. Ensures that parts of the file that contain security related information are not written during a reload. |
|--------|---------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default)#configuration-persistence secure  
RFController(config-profile-default)#
```

## controller

### *profile commands*

Configures a WLAN controller information. Sets the controller to be a part of a group of controllers, sets if the controller is a part of a pool of controllers, etc.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
controller [group <CONTROLLER-GROUP>]
controller vlan <1-4094>
controller host [<IP>|<HOSTNAME>] {[level [1|2]]/pool <1-2>]}
```

### Parameters

- |                   |                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [group host vlan] | <ul style="list-style-type: none"> <li>• group – Enter the address of the controller group to which this controller will belong</li> <li>• host – The address of the controller that is to be configured           <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Enter the IP address of the controller</li> <li>• &lt;HOSTNAME&gt; – Enter the hostname of the controller</li> </ul> </li> </ul> |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The following parameters are common to <IP> and <HOSTNAME>:

- level [1|2] – Enter the routing level. There are two routing levels you can select from. Level1 is for local routing and Level 2 is for inter-site routing
- pool <1-2> – Enter the controller pool to which this controller belongs to. Default value is 1.
- vlan <1-4094> – Enter the VLAN on which the controller can be reached. Enter a VLAN ID in the range 1 and 4094.

### Example

```
RFController(config-profile-default)#controller group test
RFController(config-profile-default-rfs7000)#controller host 1.2.3.4 pool 2
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface ge1
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
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
use firewall-policy default
controller host 1.2.3.4 pool 2
controller group test
service pm sys-restart
```

## crypto

### *profile commands*

Use crypto to define system level local ID for ISAKMP negotiation and to enter the ISAKMP Policy, ISAKMP Client or ISAKMP Peer command set.

A crypto map entry is a single policy that describes how certain traffic is secured. There are two types of crypto map entries: ipsec-manual and ipsec-ike entries. Each entry is given an index (used to sort the ordered list).

When a non-secured packet arrives on an interface, the crypto map set associated with that interface is processed (in order). If a crypto map entry matches the non-secured traffic, the traffic is discarded.

When a packet is transmitted on an interface, the crypto map set associated with that interface is processed. The first crypto map entry that matches the packet is used to secure the packet. If a suitable SA exists, it is used for transmission. Otherwise, IKE is used to establish an SA with the peer. If no SA exists (and the crypto map entry is “respond only”), the packet is discarded.

When a secured packet arrives on an interface, its SPI is used to look up a SA. If a SA does not exist (or if the packet fails any of the security checks), it is discarded. If all checks pass, the packet is forwarded normally.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
crypto [ipsec|isakmp|map|pki]

crypto ipsec [security-association|transform-set]]
crypto ipsec security-association lifetime [kilobyte|seconds] <lifetime>
crypto ipsec transform-set <transform-set-tag> [ah-md5-hmac|
ah-sha-hmac|esp-3des|esp-aes|esp-aes-192|esp-aes-256|esp-des|
esp-md5-hmac|esp-sha-hmac]

crypto isakmp [aggressive-mode-peer|client|keepalive|key|policy]]
crypto isakmp client configuration group default
crypto isakmp keepalive <10-3600>
crypto isakmp key [0 <WORD>|2 <WORD>|<WORD>] address <A.B.C.D>
[address <IP>|hostname <HOST>]
crypto isakmp aggressive-mode-peer [address <IP>|dn <distinguished-name>|
hostname <HOST>] key [0 <WORD>|2 <WORD>|<WORD>]
crypto isakmp policy <ISAKMP-POLICY>

crypto map <crypto-map-tag> <1-1000> [ipsec-isakmp|ipsec-manual] {dynamic}

crypto pki import crl <WORD> URL <1-168>
```

## Parameters

|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipsec                                                                | Configures IPSEC policies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| [security-association   transform-set]                               | <ul style="list-style-type: none"> <li>• security-association – Defines the lifetime (in kilobytes and/or seconds) of the IPsec SAs created <ul style="list-style-type: none"> <li>• lifetime [kilobyte   seconds] – Specifies how many kilobyte/seconds an IKE SA lasts before it expires. Values can be entered in both kilobytes and seconds. Which ever limit is reached first, ends the security association <ul style="list-style-type: none"> <li>• kilobytes – Volume-based key duration, the minimum is 500 KB and the maximum is 2147483646 KB</li> <li>• seconds – Time-based key duration, the minimum is 90 seconds and the maximum is 2147483646 seconds</li> </ul> </li> </ul> </li> <li>• transform-set [set name] – Uses the crypto ipsec transform-set command to define the transform configuration (authentication and encryption) for securing data <ul style="list-style-type: none"> <li>• ah-md5-hmac – AH-HMAC-MD5 transform</li> <li>• ah-sha-hmac – AH-HMAC-SHA transform</li> <li>• esp-3des – ESP transform using 3DES cipher (168 bits)</li> <li>• esp-aes – ESP transform using AES cipher</li> <li>• esp-aes-192 – ESP transform using AES cipher (192 bits)</li> <li>• esp-aes-256 – ESP transform using AES cipher (256 bits)</li> <li>• esp-des – ESP transform using DES cipher (56 bits)</li> <li>• esp-md5-hmac – ESP transform using HMAC-MD5 auth</li> <li>• esp-sha-hmac – ESP transform using HMAC-SHA auth</li> </ul> </li> </ul> <p>The transform-set is then assigned to a crypto map using the map's set transform-set command.</p> |
| isakmp<br>[aggressive-mode-peer   client   keepalive   key   policy] | <p>Configures the <i>Internet Security Association and Key Management Protocol</i> (ISAKMP) policy</p> <ul style="list-style-type: none"> <li>• aggressive-mode-peer [address   dn   hostname] – Defines the aggressive mode attributes <ul style="list-style-type: none"> <li>• address – The IP address is the identity of the remote peer</li> <li>• dn – The identity of the remote peer is the distinguished name</li> <li>• hostname –The hostname is the identity of the remote peer</li> </ul> </li> <li>• client configuration group default – Leads to the config-crypto group instance <ul style="list-style-type: none"> <li>• configuration – Defines the configuration set at the client <ul style="list-style-type: none"> <li>• group – Defines the group (currently only one is supported) <ul style="list-style-type: none"> <li>• default – Default the group tag</li> </ul> </li> </ul> </li> </ul> </li> <li>• keepalive &lt;10-3600&gt; – Sets a keepalive interval for use with remote peers. It defines the number of seconds between DPD messages.</li> <li>• key [0 2] &lt;WORD&gt; address &lt;A.B.C.D&gt; – Sets a pre-shared key for a remote peer <ul style="list-style-type: none"> <li>• 0 &lt;WORD&gt; – Enter a clear text key</li> <li>• 2 &lt;WORD&gt; – Enter an encrypted key</li> <li>• &lt;WORD&gt; –Sets a key of size minimum 8 characters</li> <li>• address &lt;A.B.C.D&gt; – Defines a shared key with an IP address</li> </ul> </li> <li>• policy &lt;ISAKMP-POLICY&gt; – Sets a policy for a ISAKMP protection suite</li> </ul>    |

---

|                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>map &lt;crypto-map-tag&gt; &lt;1-1000&gt; [ipsec-isakmp] ipsec-manual] {dynamic}</pre> | <p>Enter a crypto map</p> <ul style="list-style-type: none"> <li>• name &lt;name&gt; – Names the crypto map entry (cannot exceed 32 characters)</li> <li>• &lt;1-1000&gt; – Defines the sequence to insert into the crypto map entry <ul style="list-style-type: none"> <li>• ipsec-isakmp – IPSEC w/ISAKMP</li> <li>• ipsec-manual – IPSEC w/manual keying <ul style="list-style-type: none"> <li>• dynamic – Dynamic map entry (remote VPN configuration) for XAUTH with mode-config or ipsec-l2tp configuration</li> </ul> </li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                             |
| <pre>pki import crl &lt;WORD&gt; URL &lt;1-168&gt;</pre>                                    | <p>Configures certificate parameters. The public key infrastructure is a protocol that creates encrypted public keys using digital certificates from certificate authorities.</p> <ul style="list-style-type: none"> <li>• import – Imports a trustpoint related configuration <ul style="list-style-type: none"> <li>• crl – Certificate revocation list <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Imports a trustpoint including either a private key and server certificate or a CA certificate or both</li> </ul> </li> <li>• URL &lt;1-168&gt; – URL to get certificate from URLs: <pre>tftp://&lt;IP&gt;/path/file ftp://&lt;user&gt;:&lt;passwd&gt;@&lt;IP&gt;/path/file</pre> <ul style="list-style-type: none"> <li>• &lt;1-168&gt; – Sets the duration to replay the command (between 1 and 168 hours)</li> </ul> </li> </ul> </li> </ul> |

---

### Usage Guidelines

If no peer IP address is configured, the manual crypto map is not valid and not complete. A peer IP address is required for manual crypto maps. To change the peer IP address, the no set peer command must be issued first, then the new peer IP address can be configured.

A peer address can be deleted with a wrong ISAKMP value. Crypto currently matches only the IP address when a no command is issued.

```
RFController(config-profile-default-rfs7000)#crypto isakmp key 12345678
address 4.4.4.4
```

### Example

```
RFController(config-profile-default-rfs7000)#crypto ipsec transform-set
tpsec-tag1 ah-md5-hmac
RFController(config-profile-default-rfs7000-transform-set-tpsec-tag1)#
```

```
RFController(config-profile-default-rfs7000)#crypto map map1 10 ipsec-manual
dynamic
% Error: Remote Configuration not allowed for Manual Crypto Map
RFController(config-profile-default-rfs7000)#
```

```
RFController(config-profile-default-rfs7000)#crypto map map1 10 ipsec-isakmp
dynamic
RFController(config-profile-default-rfs7000-cryptomap-map1 10)#
```

```
RFController(config-profile-default-rfs7000)#crypto isakmp client
configuration group default
RFController(config-profile-default-rfs7000-crypto-group)#
RFController(config-profile-default-rfs7000-crypto-group)#?
Crypto Client Config commands:
  dns      Domain Name Server
  wins     Windows name server

  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
```

```
RFController(config-profile-default-rfs7000-crypto-group)#
```

## isakmp-policy

Use the (config) instance to configure ISAKMP policy related configuration commands. To navigate to the config-isakmp-policy instance, use the following commands:

```
RFController(config-profile-default-rfs7000)#crypto isakmp policy test
RFController(config-profile-default-rfs7000-isakmp-policy-test)#?
Crypto Isakmp Config commands:
 authentication Set authentication method for protection suite
 encryption      Set encryption algorithm for protection suite
 group           Set the Diffie-Hellman group
 hash           Set hash algorithm for protection suite
 lifetime        Set lifetime for ISAKMP security association
 no             Negate a command or set its defaults
 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
RFController(config-profile-default-rfs7000-isakmp-policy-test)#
```

Table 18 Summarizes isakmp-policy commands

**TABLE 18** isakmp-policy commands

| Command                        | Description                                                                                          | Reference                |
|--------------------------------|------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">authentication</a> | Authenticates rsa-sig and pre-share keys                                                             | <a href="#">page 439</a> |
| <a href="#">encryption</a>     | Configures the encryption level of the data transmitted using the <code>crypto-isakmp</code> command | <a href="#">page 440</a> |
| <a href="#">group</a>          | Specifies the Diffie-Hellman group (1 or 2) used by the IKE policy                                   | <a href="#">page 441</a> |
| <a href="#">hash</a>           | Specifies the hash algorithm                                                                         | <a href="#">page 442</a> |
| <a href="#">life-time</a>      | Specifies how long an IKE SA is valid before it expires                                              | <a href="#">page 443</a> |
| <a href="#">no</a>             | Negates a command or sets its default value                                                          | <a href="#">page 444</a> |



## *authentication*

### *isakmp-policy*

Sets the authentication method for the cryptography suite

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
authentication [pre-share|rsa-sig]
```

### **Parameters**

|           |                                               |
|-----------|-----------------------------------------------|
| pre-share | Use the pre-shared key                        |
| rsa-sig   | Use the Rivest-Shamir-Adleman (RSA) Signature |

### **Example**

```
RFController(config-isakmp-policy-test)#authentication rsa-sig
RFController(config-prfile-default-rfs7000-isakmp-policy-test)#show context
crypto isakmp policy test
authentication rsa-sig
```

## *encryption*

### *isakmp-policy*

Configures the encryption level transmitted using the `crypto-isakmp` command

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
encryption [3des|aes|aes-192|aes-256|des]
```

### **Parameters**

---

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [3des aes aes-192 <br>aes-256 des] | Sets an encryption algorithm for the protection suite <ul style="list-style-type: none"><li>• 3des - Triple data encryption standard</li><li>• aes - Advanced encryption standard (128 bit keys)</li><li>• aes-192 - Advanced encryption standard (192 bit keys)</li><li>• aes-256 - Advanced encryption standard (256 bit keys)</li><li>• des - Data encryption standard (56 bit keys)</li></ul> |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-isakmp-policy-test)#encryption 3des  
RFController(config-isakmp-policy-test)#
```

## *group*

### *isakmp-policy*

Specifies the Diffie-Hellman group (1 or 2) used by the IKE policy to generate keys (which is then used to create an IPSec SA)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
group [1|2|5]
```

### **Parameters**

---

|         |                                                                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1 2 5] | <ul style="list-style-type: none"><li>• 1- Diffie-Hellman group 1</li><li>• 2 - Diffie-Hellman group 2</li><li>• 5 - Diffie-Hellman group 5</li></ul> |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Usage Guidelines**

The local IKE policy and the peer IKE policy must have matching group settings for negotiation to be successful.

### **Example**

```
RFController(config-profile-default-rfs7000-isakmp-policy-test)#group 1
RFController(config-profile-default-rfs7000-isakmp-policy-test)#show context
crypto isakmp policy test
 authentication rsa-sig
 group 1
```

## *hash*

### *isakmp-policy*

Specifies the hash algorithm used to authenticate data transmitted over the IKE SA

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
hash [md5|sha]
```

### **Parameters**

|     |                             |
|-----|-----------------------------|
| md5 | Uses the MD5 hash algorithm |
| sha | Uses the SHA hash algorithm |

### **Example**

```
RFController(config-isakmp-policy-test)#hash sha
```

## *life-time*

### *isakmp-policy*

Specifies how long an IKE SA is valid before it expires

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
lifetime <WORD>
```

### **Parameters**

---

|                 |                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------|
| lifetime <WORD> | Specifies how many seconds an IKE SA lasts before it expires. A time stamp (in seconds) can be configured between 60 and 2147483646. |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-isakmp-policy-test)#lifetime 2000
RFController(config-profile-default-rfs7000-isakmp-policy-test)#show context
crypto isakmp policy test
  authentication rsa-sig
  group 1
  lifetime 2000
RFController(config-isakmp-policy-test)#
```

## *no*

### *isakmp-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
no [ authentication|encryption|group|hash|lifetime ]
```

### **Parameters**

---

|                                                  |                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ authentication encryption group hash lifetime] | <ul style="list-style-type: none"><li>• authentication – Sets a default authentication method</li><li>• encryption – Sets an encryption algorithm for protection suite</li><li>• group – Sets the default DH group to 2</li><li>• hash – Sets the hash algorithm for protection suite</li><li>• lifetime – Sets the lifetime for ISAKMP security association</li></ul> |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-isakmp-policy-test)#no authentication
```

```
RFController(config-isakmp-policy-test)#no lifetime
```

### **NOTE**

The commands `clscr`, `commit`, `exit`, `help`, `write`, `revert`, `service` and `show` are common commands. Refer to [Chapter 6, Common Commands](#) for more information.

---

## crypto-group

Use the (config) instance to configure crypto-group related configuration commands:

```
RFController(config-profile-default-rfs7000)#crypto isakmp client
configuration group default
RFController(config-profile-default-rfs7000-crypto-group)#
RFController(config-profile-default-rfs7000-crypto-group)#?
Crypto Client Config commands:
  dns      Domain Name Server
  wins     Windows name server

  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

RFController(config-profile-default-rfs7000-crypto-group)
```

[Table 19](#) Summarizes crypto-group commands

**TABLE 19** crypto-group commands

| Command             | Description                             | Reference                |
|---------------------|-----------------------------------------|--------------------------|
| <a href="#">dns</a> | Configures domain name server settings  | <a href="#">page 446</a> |
| <a href="#">wns</a> | Configures windows name server settings | <a href="#">page 447</a> |

### *dns*

#### *crypto-group*

Configures domain name server settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
dns <IP>
```

#### **Parameters**

---

|      |                                                |
|------|------------------------------------------------|
| <IP> | Sets the IP address for the domain name server |
|------|------------------------------------------------|

---

#### **Example**

```
RFController(config-profile-default-rfs7000-crypto-group)#dns 171.16.10.6

RFController(config-profile-default-rfs7000-crypto-group)#show context
crypto isakmp client configuration group default
wins 1.2.3.4
dns 171.16.10.6
```



## ***wns***

### *crypto-group*

Configures the Windows name server settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
wns <A.B.C.D>
```

### **Parameters**

---

|           |                                             |
|-----------|---------------------------------------------|
| <A.B.C.D> | Sets the IP address for Windows name server |
|-----------|---------------------------------------------|

---

### **Example**

```
RFController(config-profile-default-rfs7000-crypto-group)#wns 172.16.10.8
RFController(config-profile-default-rfs7000-crypto-group)#show context
crypto isakmp client configuration group default
  wins 1.2.3.4
  dns 171.16.10.6
```

## dscp-mapping

### *profile commands*

Configures IP DSCP to 802.1p priority mapping for untagged frames

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
dscp-mapping <WORD> priority <0-7>
```

### Parameters

|                |                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WORD>         | Enter a DSCP value of a received IP packet                                                                                                                      |
| priority <0-7> | Priority used for the packet if untagged. <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Specifies the 802.1p priority value between 0 and 7</li> </ul> |

### Example

```
RFController(config-profile-default-rfs7000)#dscp-mapping 20 priority 7
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  dscp-mapping 20 priority 7
  no autoinstall configuration
  no autoinstall firmware
  crypto isakmp policy default
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  interface mel
  interface gel
    ip dhcp trust
    qos trust dscp

  dscp-mapping 20 priority 7
  no autoinstall configuration
  no autoinstall firmware
  crypto isakmp policy default
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  interface mel
  interface gel
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
  interface ge2
    ip dhcp trust
    qos trust dscp
    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
use firewall-policy default
email-notification recipient test@brocade.com
service pm sys-restart
```

## email-notification

### *profile commands*

Configures email notification

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
email-notification [host <IP>|recipient <EMAIL>]
email-notification host <IP> sender <EMAIL> {port <1-65535>/|username <WORD>}
```

### Parameters

---

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [host recipient]]            | • host <IP>- Configures the host SMTP server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| host[sender {port username}] | <ul style="list-style-type: none"> <li>• &lt;IP&gt; - The IP address of the SMTP server.</li> <li>• sender &lt;EMAIL&gt; - configures sender email address           <ul style="list-style-type: none"> <li>• &lt;EMAIL&gt; - Enter the email address of the sender</li> <li>• port - Optional. Enter the port number. The port number can be within 1-65535</li> <li>• username - Optional. Enter the SMTP user name</li> </ul> </li> <li>• recipient &lt;EMAIL&gt; - Configures the address of recipient email address           <ul style="list-style-type: none"> <li>• &lt;EMAIL&gt; - Enter the email address of the recipient</li> </ul> </li> </ul> |

---

### Example

```
RFController(config-profile-default)#email-notification recipient
test@brocade.com
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
dscp-mapping 20 priority 7
no autoinstall configuration
no autoinstall firmware
crypto isakmp policy default
crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
interface me1
interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
interface ge2
  ip dhcp trust
  qos trust dscp
  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
use firewall-policy default
email-notification recipient test@brocade.com
service pm sys-restart
```

## enforce-version

### *profile commands*

Checks the firmware versions of devices before interoperating

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
enforce-version [adoption|cluster] [full|major|none|strict]
```

### Parameters

[adoption|cluster]

- adoption – Checks the firmware versions before adopting
- cluster – Checks the firmware versions before clustering

The following parameters are common to adoption and cluster:

- full – Allows adoption/clustering only when full versions of the firmware are exactly the same
- major – Allows adoption/clustering only when major and minor versions are exactly the same
- none – Allows adoption/clustering between any version
- strict – Allows adoption/clustering when firmware versions are exactly the same

### Example

```
RFController(config-profile-default)#enforce-version cluster full
RFController(config-profile-default)#enforce-version adoption major
RFController(config-profile-default-rfs7000)#show context
profile rfs7000 default-rfs7000
  dscp-mapping 20 priority 7
  no autoinstall configuration
  no autoinstall firmware
  crypto isakmp policy default
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  interface me1
  interface ge1
    ip dhcp trust
    qos trust dscp
    qos trust 802.1p
  interface ge2
    ip dhcp trust
    qos trust dscp
    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
use firewall-policy default
email-notification recipient test@brocade.com
enforce-version adoption major
enforce-version cluster full
service pm sys-restart
```

## events

### *profile commands*

Displays system event messages

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
events [forward on|on]
```

### Parameters

---

|                 |                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [forward on on] | <ul style="list-style-type: none"><li>• forward – Forwards system event messages to the wireless controller or cluster member s<ul style="list-style-type: none"><li>• on – Enables the forwarding of system events</li></ul></li><li>• on – Generates system events on this controller</li></ul> |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs7000)#events forward on  
RFController(config-profile-default-rfs7000)#
```



## ip

### *profile commands*

Configures a selected Internet Protocol component

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ip [ default-gateway | dns-server-forward | route | dhcp | domain-lookup |
domain-name | local | name-server | nat | routing ]
ip dhcp client [ hostname | persistent-lease ]
ip default-gateway <A.B.C.D>
ip route <A.B.C.D/M> <A.B.C.D>
ip domain-name <WORD>
ip local pool default low-ip-address <A.B.C.D> { high-ip-address } <A.B.C.D>
ip name-server <A.B.C.D>
ip nat [ inside | outside | pool ]
ip nat [ inside | outside ] [ destination | source ]
ip nat [ inside | outside ] [ destination static <A.B.C.D> [ <1-65535> [ [ tcp | udp ]
<A.B.C.D> { 1-65535 } ] ] | <A.B.C.D> { 1-65535 } ]
ip nat [ inside | outside ] [ source [ list <IP-ACCESS-LIST> interface vlan
<1-4094> [ address <A.B.C.D> overload | overload | pool <NAT-pool>
overload ] | static <A.B.C.D> <A.B.C.D> ]
ip nat pool <NAT-POOL> prefix-length <1-30>
```

## Parameters

|                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default-gateway <A.B.C.D>                                                        | Configures the IP address of the default gateway <ul style="list-style-type: none"> <li>&lt;A.B.C.D&gt; – IP address of the next-hop router</li> </ul>                                                                                                                                                                                                                                                                                                                                    |
| dns-server-forward                                                               | Enables <i>Domain Name Service (DNS) Forwarding</i>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| route <A.B.C.D/M> <A.B.C.D>                                                      | Establishes static routes <ul style="list-style-type: none"> <li>&lt;A.B.C.D/M&gt; – IP destination prefix (e.g. 10.0.0.0/8)</li> <li>&lt;A.B.C.D&gt; – IP gateway address</li> </ul>                                                                                                                                                                                                                                                                                                     |
| dhcp client<br>[hostname   persistent-lease]                                     | Configures the <i>Dynamic Host Control Protocol (DHCP)</i> client and host <ul style="list-style-type: none"> <li>client – Sets the DHCP client <ul style="list-style-type: none"> <li>hostname – Includes the hostname in the DHCP request</li> <li>persistent-lease – Retains last lease across reboot if DHCP server is unreachable</li> </ul> </li> </ul>                                                                                                                             |
| domain-lookup                                                                    | Enables domain lookup service                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| domain-name <WORD>                                                               | Configures a default domain name for DNS                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| local pool default low-ip-address<br><A.B.C.D> {highest-ip-address}<br><A.B.C.D> | Sets an IP address range assigned to VPN clients using mode-config or IPsec with L2TP <ul style="list-style-type: none"> <li>pool default – Specifies the address range to configure <ul style="list-style-type: none"> <li>default – Default group tag <ul style="list-style-type: none"> <li>low-ip-address &lt;A.B.C.D&gt; – Sets lowest range for IP address</li> <li>{highest-ip-address} &lt;A.B.C.D&gt; – Sets the highest range for IP address</li> </ul> </li> </ul> </li> </ul> |
| name-server <A.B.C.D>                                                            | Configures the IP address of the name-server                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> nat [inside   outside][destination static &lt;A.B.C.D&gt; [&lt;1-65535&gt;[[tcp   udp] &lt;A.B.C.D&gt; {1-65535}]]   &lt;A.B.C.D&gt; {1-65535}]] source [list &lt;IP-ACCESS-LIST&gt; interface vlan &lt;1-4094&gt; [&lt;A.B.C.D&gt; overload   overload]] static &lt;A.B.C.D&gt; &lt;A.B.C.D&gt;] </pre> | <p><i>Network Address Translation (NAT)</i></p> <ul style="list-style-type: none"> <li>inside – Inside address translation</li> <li>outside – Outside address translation</li> </ul> <p>The following parameters are the same for both inside and outside NAT parameters:</p> <ul style="list-style-type: none"> <li>destination static – Specifies the destination address translation to configure <ul style="list-style-type: none"> <li>static &lt;A.B.C.D&gt; – Specifies the static NAT mapping <ul style="list-style-type: none"> <li>&lt;A.B.C.D&gt; [&lt;1-65535&gt;   &lt;A.B.C.D&gt;] – Specifies the IP address (A.B.C.D) to configure <ul style="list-style-type: none"> <li>&lt;1-65535&gt; [tcp   udp] – Select a value between 1 and 65535 to configure as an actual outside port</li> <li>tcp – Transmission control protocol</li> <li>udp – User datagram protocol</li> </ul> </li> </ul> </li> </ul> </li> </ul> <p>The following parameters are common for both TCP and UDP:</p> <ul style="list-style-type: none"> <li>&lt;A.B.C.D&gt; {&lt;1-65535&gt;} – Specifies the outside natted IP address (A.B.C.D) to configure</li> <li>&lt;1-65535&gt; – Select a value between 1 and 65535 to configure outside natted port</li> <li>A.B.C.D&gt; &lt;1-65535&gt; – Specifies the outside natted IP address (A.B.C.D)</li> <li>&lt;1-65535&gt; – Select a value between 1 and 65535 to configure outside natted Port</li> </ul> <ul style="list-style-type: none"> <li>source – Specifies the source address translation to configure <ul style="list-style-type: none"> <li>list &lt;IP-ACCESS-LIST&gt; – Specifies the access list describing local addresses <ul style="list-style-type: none"> <li>&lt;IP-ACCESS-LIST&gt; interface – Specifies the access list name</li> <li>interface vlan – Select an Interface to configure</li> <li>vlan &lt;1-4094&gt; – Select a VLAN interface (switched virtual interface) to configure</li> <li>&lt;1-4094&gt; [address &lt;A.B.C.D&gt; overload   overload   pool] – Select a VLAN ID between 1 and 4094 to configure the interface</li> <li>address &lt;A.B.C.D&gt; overload – Specifies an interface IP address used for NAT</li> <li>overload – Enables the use of one global address for numerous local addresses.</li> <li>pool &lt;NAT-POOL&gt; overload – Sets the NAT pool</li> <li>&lt;NAT-POOL&gt; – Specifies the NAT pool</li> </ul> </li> <li>static [&lt;A.B.C.D&gt;   &lt;A.B.C.D&gt;] – Specifies the static local-global mapping <ul style="list-style-type: none"> <li>&lt;A.B.C.D&gt; – Specifies the inside actual IP address (A.B.C.D) to configure</li> <li>A.B.C.D&gt; – Specifies the natted IP address (A.B.C.D) to configure</li> </ul> </li> </ul> </li> <li>pool &lt;NAT-POOL&gt; – IP address pool for NAT <ul style="list-style-type: none"> <li>&lt;NAT-POOL&gt; – Specifies the NAT pool to use</li> <li>prefix-length &lt;1-30&gt; – Specifies the number of netmask bits</li> </ul> </li> </ul> |
| <pre> routing </pre>                                                                                                                                                                                                                                                                                           | <p>Enables IP routing</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Example

```

RFController(config-profile-default-rfs7000)#ip default-gateway 172.16.10.9
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#ip dns-server-forward
RFController(config-profile-default-rfs7000)#
RFController(config-profile-default-rfs7000)#ip route 172.16.10.10/24
172.16.10.2
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#ip local pool default
low-ip-address 1.2.3.4 high-ip-address 6.7.8.9
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#ip nat inside source list test
interface vlan 1 pool pool1 overload
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#ip nat pool pool1 prefix-length 9
RFController(config-profile-default-rfs7000-nat-pool-pool1)#
RFController(config-profile-default-rfs7000-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

RFController(config-profile-default-rfs7000-nat-pool-pool1)

```

## nat-pool

Use this (config-profile-default-rfs7000) instance to configure NAT pool commands.

```
RFController(config-profile-default-rfs7000)#ip nat pool pool1 prefix-length
RFController(config-profile-default-rfs7000-nat-pool-pool1)#ip nat pool pool1
prefix-length 1
RFController(config-profile-default-rfs7000-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
RFController(config-profile-default-rfs7000-nat-pool-pool1)
```

[Table 20](#) Summarizes nat-pool commands

**TABLE 20** nat-pool commands

| Command                 | Description                           | Reference                |
|-------------------------|---------------------------------------|--------------------------|
| <a href="#">address</a> | Specifies addresses for the NAT pool  | <a href="#">page 460</a> |
| <a href="#">no</a>      | Negates a command or sets its default | <a href="#">page 461</a> |

## *address*

### *nat-pool commands*

Specifies IP addresses for the nat pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
address [<IP>|range]
address range <Start-IP> <End-IP>
```

### **Parameters**

- 
- |                                    |                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP> range <Start-IP><br><End-IP>] | <ul style="list-style-type: none"><li>• &lt;IP&gt; - Specifies a single IP address to add to the NAT pool</li><li>• range - Specifies an address range to configure<ul style="list-style-type: none"><li>• &lt;Start-IP&gt; - Specifies the starting IP address</li><li>• &lt;End-IP&gt; - Specifies the ending IP address</li></ul></li></ul> |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

### **Example**

```
RFController(config-profile-default-rfs7000-nat-pool-pool1)#address range
172.16.10.2 172.16.10.8
```

***no******nat-pool commands***

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no address
```

**Parameters**

None

**Usage Guidelines**

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

**Example**

```
RFCcontroller(config-profile-default-rfs7000-nat-pool-pool1)#no address
```

## interface

### *profile commands*

Selects an interface to configure

This command is used to enter the interface configuration mode for the specified physical controller *Virtual Interface* (SVI) interface. If the VLANs (SVI) interface does not exist, it's automatically created.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
interface [ <WORD> | fe <1-4> | ge<1-8> | me1 | port-channel<1-8> | radio
<1-3> | up1 | vlan<1-4094> | wwan1 ]
```

### Parameters

|                    |                                                                                                          |
|--------------------|----------------------------------------------------------------------------------------------------------|
| <WORD>             | Defines the name of the interface selected                                                               |
| fe <1-4>           | Fast Ethernet interface                                                                                  |
| ge <1-8>           | Gigabit Ethernet interface (4 for the Mobility RFS7000 Controller and 8 for Mobility RFS6000 Controller) |
| me1                | Management interface<br>Not applicable for Mobility RFS4000 Controller                                   |
| port-channel <1-8> | Select a port channel interface between 1 and 8                                                          |
| radio <1-3>        | Select a radio between 1 and 3                                                                           |
| up1                | Uplink Gigabit Ethernet interface (Mobility RFS6000 Controller and Mobility RFS7000 Controller only)     |
| vlan <1-4094>      | Defines the VLAN interface                                                                               |
| wwan1              | Defines the wireless WAN interface                                                                       |



**Example**

```
RFController(config-profile-default-rfs7000)#interface vlan 44
RFController(config-profile-default-rfs7000-if-vlan44)#?
VLAN configuration commands:
allow-management      Allow management
crypto                Encryption module
description           Vlan description
dhcp-relay-incoming  Allow on-board DHCP server to respond to relayed DHCP
                    packets on this interface
ip                    Interface Internet Protocol config commands
no                    Negate a command or set its defaults
shutdown             Shutdown the selected interface
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

RFController(config-profile-default-rfs7000-if-vlan8)#
```

## Interface Config Instance

Use the (config-profile-default-rfs7000) instance to configure the interfaces – Ethernet, VLAN and tunnel associated with the controller.

To switch to this mode, use the following command:

```
RFController(config-profile-default-rfs7000)#interface
[<interface-name>|fe<1-4>|ge <1-4>|me1|port-channel <1-4>|radio|up1|vlan
<1-4094>|wwan1]
RFController(config-profile-default-rfs7000)# ge 1
RFController(config-profile-default-rfs7000-if-ge1)#?
Interface Config commands:
```

|               |                                                   |
|---------------|---------------------------------------------------|
| cdp           | Enable Cisco Discovery Protocol on port           |
| channel-group | Channel group commands                            |
| description   | Interface specific description                    |
| dot1x         | 802.1X Authentication                             |
| duplex        | Set duplex to interface                           |
| ip            | Internet Protocol (IP)                            |
| no            | Negate a command or set its defaults              |
| power         | PoE Command                                       |
| qos           | Quality of service                                |
| 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 |

```
RFController(config-profile-default-rfs7000-if-ge1)#
```

Table 21 Summarizes the Interface Config Commands

**TABLE 21** interface config commands

| <b>Command</b>       | <b>Description</b>                                                                       | <b>Reference</b>         |
|----------------------|------------------------------------------------------------------------------------------|--------------------------|
| <i>cdp</i>           | Enables the <i>Cisco Discovery Protocol</i> (CDP) on ports                               | <a href="#">page 466</a> |
| <i>channel-group</i> | Configures channel-group commands                                                        | <a href="#">page 467</a> |
| <i>description</i>   | Creates an interface specific description                                                | <a href="#">page 468</a> |
| <i>dot1x</i>         | Configures 802.1X authentication settings                                                | <a href="#">page 469</a> |
| <i>duplex</i>        | Specifies the duplex mode for the interface                                              | <a href="#">page 470</a> |
| <i>ip</i>            | Sets the IP address for the assigned Fast Ethernet interface (ME), and VLAN Interface    | <a href="#">page 471</a> |
| <i>lldp</i>          | Configures Link Local Discovery Protocol                                                 | <a href="#">page 472</a> |
| <i>no</i>            | Negates a command or sets its defaults                                                   | <a href="#">page 473</a> |
| <i>power</i>         | Invokes PoE commands to configure the PoE power limit and port priority                  | <a href="#">page 474</a> |
| <i>qos</i>           | Enables quality of service                                                               | <a href="#">page 475</a> |
| <i>shutdown</i>      | Disables the selected interface                                                          | <a href="#">page 476</a> |
| <i>spanning-tree</i> | Configures spanning tree parameters                                                      | <a href="#">page 477</a> |
| <i>speed</i>         | Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000) | <a href="#">page 480</a> |
| <i>switchport</i>    | Sets switching mode characteristics for a selected interface                             | <a href="#">page 481</a> |
| <i>use</i>           | Defines the settings to use with this command                                            | <a href="#">page 483</a> |

### *cdp*

#### *interface config commands*

Enables the Cisco Discovery Protocol (CDP) on the controller ports

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
cdp [transmit|receive]
```

#### **Parameters**

- 
- |                    |                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| [transmit receive] | <ul style="list-style-type: none"><li>• receive – Enables snooping of CDP packets</li><li>• transmit – Enables transmission of CDP packets</li></ul> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

#### **Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#cdp transmit  
RFController(config-profile-default-rfs7000-if-ge1)#
```

## *channel-group*

### *interface config commands*

Configures channel-group commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
channel-group <1-5>
```

### **Parameters**

---

|       |                                                          |
|-------|----------------------------------------------------------|
| <1-5> | Specifies a group number for channel-group configuration |
|-------|----------------------------------------------------------|

---

### **Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#channel-group 1
RFController(config-profile-default-rfs7000-if-ge1)#
```

### *description*

#### *interface config commands*

Creates an interface specific description

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
description [<LINE>|<WORD>]
```

#### **Parameters**

---

|                 |                                                  |
|-----------------|--------------------------------------------------|
| [<LINE> <WORD>] | Defines the characters describing this interface |
|-----------------|--------------------------------------------------|

---

#### **Example**

```
RFController(config-profile-default-rfs7000-if-gel)#description "interface  
for Retail King"  
RFController(config-profile-default-rfs7000-if-gel)#
```

## *dot1x*

### *interface config commands*

Configures 802.1X authentication settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dot1x [username <WORD>|password [0 <WORD>|2 <WORD>|<WORD>]
```

### **Parameters**

---

|                           |   |                                                        |
|---------------------------|---|--------------------------------------------------------|
| [username <WORD> password | • | username <WORD> - Sets the username for authentication |
| [0 <WORD>  2              | • | password [0 2 <WORD>] - Sets the password              |
| <WORD> <WORD>]            |   | • 0 - Enter a clear text password                      |
|                           |   | • 2 - Enter an encrypted password                      |
|                           |   | • <WORD> - Defines the password                        |

---

### **Example**

```
RFController(config-profile-default-rfs7000-if-gel)#dot1x username Bob
password brocade
RFController(config-profile-default-rfs7000-if-gel)#
```

### *duplex*

#### *interface config commands*

Specifies the duplex mode for the interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

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

#### **Parameters**

---

|                  |                                                                                                                                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [auto half full] | <ul style="list-style-type: none"><li>• auto – Sets the ports duplexity automatically. The port automatically detects whether it should run in full or half-duplex mode</li><li>• half – Sets the port to half-duplex mode</li><li>• full – Sets the port to full-duplex mode</li></ul> |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

#### **Example**

```
RFController(config-profile-default-rfs7000-if-gel)#duplex auto  
RFController(config-profile-default-rfs7000-if-gel)#
```



*ip**interface config commands*

Sets the IP address for the assigned Fast Ethernet interface (ME), and VLAN interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

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

**Parameters**


---

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [arp dhcp] | <ul style="list-style-type: none"> <li>• arp [header-mismatch-validation   trust] – Sets ARP for the packets             <ul style="list-style-type: none"> <li>• header-mismatch-validation – Verifies the mismatch for source MAC address in ARP header and ethernet header</li> <li>• trust – Sets the ARP trust state for ARP responses on this interface</li> </ul> </li> <li>• dhcp trust – Uses a DHCP Client to obtain an IP address for the interface (this enables DHCP on a Layer 3 SVI)             <ul style="list-style-type: none"> <li>• trust – Sets the DHCP trust state for DHXP responses on this interface</li> </ul> </li> </ul> |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#ip dhcp trust
RFController(config-profile-default-rfs7000-if-ge1)#
```

### *lldp*

#### *interface config commands*

Configures Link Local Discovery Protocol

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
lldp [receive|transmit]
```

#### **Parameters**

- 
- |                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| [receive transmit] | <ul style="list-style-type: none"><li>• receive – Enables snooping of LLDP PDUs</li><li>• transmit – Enables transmissions of LLDP PDUs</li></ul> |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
- 

#### **Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#lldp transmit  
RFController(config-profile-default-rfs7000-if-ge1)#
```

## *no*

### *interface config commands*

Negates a command or sets its defaults

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
no [ arp | cdp | channel-group | description | dot1k | duplex | ip | lldp | power | qos |  
shutdown | spanning-tree | speed | switchport | use ]
```

### **Parameters**

None

### **Usage Guidelines**

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

### **Example**

```
RFController(config-profile-default-rfs7000-if-gel)#no cdp  
RFController(config-profile-default-rfs7000-if-gel)#  
  
RFController(config-profile-default-rfs7000-if-gel)#no duplex  
RFController(config-profile-default-rfs7000-if-gel)#
```

***power******interface config commands***

Invokes PoE commands to configure the PoE power limit and port priority. By default, the value for a GE port is set to low. Power is applied in order of priority, power overloads are removed in the reverse order of priority.

Supported in the following platforms:

- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**NOTE**

This command is not supported on the Mobility RFS7000 Controller.

**Syntax**

```
power {limit <0-40>/priority}
power priority [critical|high|low]
```

**Parameters**

|                              |                                                                                                                                                                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| limit <0-40>                 | Sets the power limit on the given port to the stated power in Watts. Select the power limit value between 0-40 (Watts). It actually limits to 29.7W                                                                                                        |
| priority [critical high low] | Sets PoE priority for port <ul style="list-style-type: none"> <li>• critical – Sets the PoE priority as a critical priority</li> <li>• high – Sets the PoE priority as a high priority</li> <li>• low – Sets the PoE priority as a low priority</li> </ul> |

**Usage Guidelines**

Use [no] power to rollback the PoE configurations and set back the default configuration

**Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#power priority critical
% Error: No POE support on device type [rfs7000].
RFController(config-profile-default-rfs7000-if-ge1)#
```

## *qos*

### *interface config commands*

Enables *quality of service* (QoS)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

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

### **Parameters**

---

|                         |                                                                                                                                                                                                                                                                                                                              |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| trust [802.1p cos dscp] | Trust QoS values ingressing on interface <ul style="list-style-type: none"><li>• 802.1p - Sets the trust 802.1p COS values ingressing on the interface</li><li>• cos - Sets the trust 802.1p COS values ingressing on the interface</li><li>• dscp - Sets the trust IP DSCP QoS values ingressing on the interface</li></ul> |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#qos trust dscp  
RFController(config-profile-default-rfs7000-if-ge1)#
```

### *shutdown*

#### *Interface Config Instance*

Disables the selected interface, the interface is administratively enabled unless explicitly disabled using this command.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
shutdown
```

#### **Parameters**

None

#### **Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#shutdown  
RFController(config-profile-default-rfs7000-if-ge1)#
```

## *spanning-tree*

### Interface Config Instance

Configures spanning tree parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point

### Syntax

```
spanning-tree [bpdufilter|bpduguard|edgeport|force-version <0-3>|
guard root|link-type|mst|port-cisco-interopability |portfast]
spanning-tree [bpdufilter|bpduguard] [disable|enable]
spanning-tree link-type [point-to-point|shared]
spanning-tree mst <0-15> [cost <1-200000000>|port-priority <0-240>]
spanning-tree port-cisco-interopability [disable|enable]
```

### Parameters

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bpdufilter [disable enable]          | Use this command to set a portfast BPDU filter for the port. Use the <code>no</code> parameter with this command to revert the port BPDU filter to its default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFast enabled ports do not transmit or receive BPDUs.                                                                                                                                                                                                                                                                           |
| bpduguard [disable enable]           | Use this command to enable or disable the BPDU guard feature on a port. Use the <code>no</code> parameter with this command to set the BPDU guard feature to its default values.<br><br>When the BPDU guard is set for a bridge, all portfast-enabled ports that have the BPDU-guard set to default shut down the port upon receiving a BPDU. If this occurs, the BPDU is not processed. The port can be brought back either manually (using the <code>no shutdown</code> command), or by configuring the <code>errdisable-timeout</code> to enable the port after the specified interval. |
| edgeport                             | Enables an interface as an edge port                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| force-version <0-3>                  | Specifies the spanning-tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: <ul style="list-style-type: none"> <li>• 0 – STP</li> <li>• 1 – Not supported</li> <li>• 2 – RSTP</li> <li>• 3 – MSTP</li> </ul> The default value for forcing the version is MSTP                                                                                                                                                                                                                                                 |
| guard root                           | Enables the Root Guard feature for the port. The Root Guard disables the reception of superior BPDUs.<br><br>The Root Guard ensures the enabled port is a designated port. If the Root Guard enabled port receives a superior BPDU, it moves to a discarding state. Use the <code>no</code> parameter with this command to disable the Root Guard feature.                                                                                                                                                                                                                                 |
| link-type<br>[point-to-point shared] | Enables or disables point-to-point or shared link types <ul style="list-style-type: none"> <li>• point-to-point – Enables rapid transition</li> <li>• shared – Disables rapid transition</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |

## 8 Creating profiles

---

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mst [<0-15><br>[cost <1-200000000> <br>port-priority <0-240> | Configures MST values on a spanning tree <ul style="list-style-type: none"><li>• &lt;0-15&gt; [cost &lt;1-200000000&gt; port-priority &lt;0-240&gt;] – Defines the Instance ID<ul style="list-style-type: none"><li>• cost &lt;1-200000000&gt; – Defines the path cost for a port</li><li>• port-priority &lt;0-240&gt; – Defines the port priority for a bridge</li></ul></li></ul> |
| port-cisco-interoperability<br>[disable enable]              | Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP). <ul style="list-style-type: none"><li>• enable – Enables CISCO Interoperability</li><li>• disable – Disables CISCO Interoperability - The default value is disabled</li></ul>                                                                                          |
| portfast                                                     | Enables rapid transitions                                                                                                                                                                                                                                                                                                                                                            |

---



**Example**

```
RFController(config-profile-default-rfs7000-if-gel)#spanning-tree bpdudfilter
disable
RFController(config-profile-default-rfs7000-if-gel)#

RFController(config-profile-default-rfs7000-if-gel)#spanning-tree bpduguard
enable
RFController(config-profile-default-rfs7000-if-gel)#

RFController(config-profile-default-rfs7000-if-gel)#spanning-tree
force-version 1
RFController(config-profile-default-rfs7000-if-gel)#

RFController(config-profile-default-rfs7000-if-gel)#spanning-tree guard root
RFController(config-profile-default-rfs7000-if-gel)#

RFController(config-profile-default-rfs7000-if-gel)#spanning-tree mst 2
port-priority 10
RFController(config-profile-default-rfs7000-if-gel)#

RFController(config-profile-default-rfs7000-if-gel)#show context
interface gel
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1
  spanning-tree link-type shared
  spanning-tree bpduguard enable
  spanning-tree bpdudfilter enable
  spanning-tree force-version 1
  spanning-tree guard root
  spanning-tree mst 2 port-priority 10
  spanning-tree mst 2 cost 200
  qos trust 802.1p
RFController(config-profile-default-rfs7000-if-gel)#
```

***speed******Interface Config Instance***

Specifies the speed of a fast-ethernet (10/100) or a gigabit-ethernet port (10/100/1000)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point

**Syntax**

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

**Parameters**

|      |                                                                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10   | Forces 10 Mbps operation                                                                                                                                                                |
| 100  | Forces 100 Mbps operation                                                                                                                                                               |
| 1000 | Forces 1000 Mbps operation                                                                                                                                                              |
| auto | Port automatically detects the speed it should run based on the port at the other end of the link. Auto negotiation is a requirement for using 1000BASE-T[3] according to the standard. |

**Usage Guidelines**

Set the interface speed to auto detect and use the fastest speed available. Speed detection is based on connected network hardware

**Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#speed 10
RFController(config-profile-default-rfs7000-if-ge1)#

RFController(config-profile-default-rfs7000-if-ge1)#speed auto
RFController(config-profile-default-rfs7000-if-ge1)#
```

## *switchport*

### *Interface Config Instance*

Sets switching mode characteristics for the selected interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

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

**Parameters**

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access vlan &lt;1-4094&gt;</code> | Configures the access VLAN of an access-mode port <ul style="list-style-type: none"> <li><code>vlan &lt;1-4094&gt;</code> – Sets the VLAN when interface is in access mode</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>mode [access trunk]</code>        | Sets the mode of the interface to access or trunk mode (can only be used on physical (layer2) interfaces) <ul style="list-style-type: none"> <li><code>access</code> – If access mode is selected, the access VLAN is automatically set to <code>vlan1</code>. In this mode, only untagged packets in the access VLAN (<code>vlan1</code>) are accepted on this port. All tagged packets are discarded</li> <li><code>trunk</code> – If trunk mode is selected, tagged VLAN packets VLANs are accepted. The native vlan is automatically set to <code>VLAN1</code>. Untagged packets are placed in the native VLAN by the controller. Outgoing packets in the native VLAN are sent untagged. <code>trunk</code> is the default mode for both ports.</li> </ul>                                                                                                                                                                                                                                                                                                                                                  |
| <code>trunk [allowed  native]</code>    | Sets the trunking mode characteristics <ul style="list-style-type: none"> <li><code>allowed vlan</code> – Configures trunk characteristics when the port is in trunk-mode</li> <li><code>vlan [add  none  remove]</code> – Sets allowed VLANs <ul style="list-style-type: none"> <li><code>none</code> – Allows no VLANs to Xmit/Rx through the Layer2 interface</li> <li><code>add &lt;vlan-id&gt;</code> – Adds VLANs to the current list</li> <li><code>remove &lt;VLAN-ID&gt;</code> – Removes VLANs from the current list <ul style="list-style-type: none"> <li><code>&lt;VLAN-ID&gt;</code> – VLAN IDs added or removed. Can be either a range of VLAN (55-60) or a list of comma separated IDs (35, 41 etc.)</li> </ul> </li> </ul> </li> <li><code>native [tagged vlan &lt;1-4094&gt;]</code> – Configures the native VLAN ID of the trunk-mode port <ul style="list-style-type: none"> <li><code>tagged</code> – Tags the native VLAN</li> <li><code>vlan &lt;1-4094&gt;</code> – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode</li> </ul> </li> </ul> |

**Usage Guidelines**

Interfaces `ge1-ge4` can be configured as trunk or in access mode. An interface (when configured as trunk) allows packets (from the given list of VLANs) to be added to the trunk. An interface configured as “access” allows packets only from native VLANs

Use the `[no] switchport (access|mode|trunk)` to undo switchport configurations

**Example**

```
RFController(config-profile-default-rfs7000-if-ge1)#switchport trunk native
tagged
RFController(config-profile-default-rfs7000-if-ge1)#

RFController(config-profile-default-rfs7000-if-ge1)#switchport access vlan 1
RFController(config-profile-default-rfs7000-if-ge1)#
```

**use****Interface Config Instance**

Defines the settings used with this command

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

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

**Parameters**


---

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list in<br><IP-ACCESS-LIST> <br>mac-access-list in<br><MAC-ACCESS-LIST>] | <ul style="list-style-type: none"> <li>• ip-access-list – Uses an IP access list <ul style="list-style-type: none"> <li>• in – Applies ACL on incoming packets <ul style="list-style-type: none"> <li>• &lt;IP-ACCESS-LIST&gt; – Specifies the IP access name to use with the list</li> </ul> </li> </ul> </li> <li>• mac-access-list – Uses a MAC access list <ul style="list-style-type: none"> <li>• in – Applies ACL on incoming packets <ul style="list-style-type: none"> <li>• &lt;MAC-ACCESS-LIST&gt; – Specifies the MAC access list name</li> </ul> </li> </ul> </li> </ul> |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-profile-default-rfs7000-if-gel)#use mac-access-list in
test
RFController(config-profile-default-rfs7000-if-gel)#
```

## Interface vlan Instance

Use the (config-profile-default-rfs7000) instance to configure interfaces – Ethernet, VLAN and the tunnel associated with the controller.

To switch to this mode, use the command:

```
RFController(config-profile-default-rfs7000)#interface [<interface-name>|ge
<1-4>|me1|port-channel <1-4>|radio|up1|vlan <1-4094>]
RFController(config-profile-default-rfs7000)#vlan 8
RFController(config-profile-default-rfs7000-if-vlan8)#
```

[Table 22](#) Summarizes interface vlan mode commands

**TABLE 22** interface vlan mode commands

| Commands                            | Description                                                                         | Reference                |
|-------------------------------------|-------------------------------------------------------------------------------------|--------------------------|
| <a href="#">crypto</a>              | Defines the encryption module                                                       | <a href="#">page 485</a> |
| <a href="#">description</a>         | Defines the VLAN description                                                        | <a href="#">page 486</a> |
| <a href="#">dhcp-relay-incoming</a> | Allows an on-board DHCP server to respond to relayed DHCP packets on this interface | <a href="#">page 487</a> |
| <a href="#">ip</a>                  | Configures Internet Protocol (IP) config commands                                   | <a href="#">page 488</a> |
| <a href="#">no</a>                  | Negates a command or sets its default                                               | <a href="#">page 489</a> |
| <a href="#">shutdown</a>            | Shuts down the selected interface                                                   | <a href="#">page 490</a> |
| <a href="#">use</a>                 | Defines the settings used with this command                                         | <a href="#">page 491</a> |

## *crypto*

### *interface vlan mode commands*

Sets the encryption module to use for this interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

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

### **Parameters**

---

|                  |                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------|
| map <CRYPTO-MAP> | Attaches a crypto map to the VLAN                                                             |
|                  | <ul style="list-style-type: none"><li>• &lt;CRYPTO-MAP&gt; - Specifies the map name</li></ul> |

---

### **Example**

```
RFController(config-profile-default-rfs7000-if-vlan8)#crypto map map1
RFController(config-profile-default-rfs7000-if-vlan8)#
```

### *description*

#### *interface vlan mode commands*

Defines a description for the VLAN interface. Use this command to provide additional information about the VLAN.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
description <WORD>
```

#### **Parameters**

---

|                    |                              |
|--------------------|------------------------------|
| description <WORD> | Defines the VLAN description |
|--------------------|------------------------------|

---

#### **Example**

```
RFController(config-profile-default-rfs7000-if-vlan44)#description brocade
RFController(config-profile-default-rfs7000-if-vlan44)#
```



## *dhcp-relay-incoming*

### *interface vlan mode commands*

Allows an on board DHCP server to respond to relayed DHCP packets on this interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dhcp-relay-incoming
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default-rfs7000-if-vlan8)#dhcp-relay-incoming  
RFController(config-profile-default-rfs7000-if-vlan8)#
```

*ip**interface vlan mode commands*

Configures Internet Protocol (IP) config commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
ip [address|dhcp|helper-address <A.B.C.D>|nat]
ip address [<A.B.C.D/M> {secondary}|dhcp|zeroconfig {secondary} ]
ip nat [inside|outside]
ip dhcp client request options all]
```

**Parameters**

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| address [<A.B.C.D/M> {secondary} dhcp] | Sets the IP address of an interface <ul style="list-style-type: none"> <li>• &lt;A.B.C.D/M &gt; - Specifies the IP address (e.g. 10.0.0.1/8)               <ul style="list-style-type: none"> <li>• secondary - Specifies a secondary IP address</li> </ul> </li> <li>• dhcp - Uses a DHCP client to obtain an IP address for this interface</li> </ul>                                                                                                      |
| dhcp client request options all        | Uses a DHCP client to configure the request <ul style="list-style-type: none"> <li>• client - DHCP client               <ul style="list-style-type: none"> <li>• request - Configures the request                   <ul style="list-style-type: none"> <li>• options - DHCP options                       <ul style="list-style-type: none"> <li>• all - Configures all the DHCP options based on the request</li> </ul> </li> </ul> </li> </ul> </li> </ul> |
| helper-address <A.B.C.D>               | Forwards DHCP and BOOTP packets <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; - Specifies the IP for DHCP and BOOTP packet forwarding</li> </ul>                                                                                                                                                                                                                                                                                                  |
| nat [inside outside]                   | Sets the <i>Network Address Translation</i> (NAT) of an interface <ul style="list-style-type: none"> <li>• inside - Inside interface</li> <li>• outside - Outside interface</li> </ul>                                                                                                                                                                                                                                                                       |

**Example**

```
RFController(config-profile-default-rfs7000-if-vlan44)#ip nat inside
RFController(config-profile-default-rfs7000-if-vlan44)#

RFController(config-profile-defalut-rfs7000-if-vlan2)#ip address 10.0.0.1/8
RFController(config-profile-defalut-rfs7000-if-vlan2)#

RFController(config-profile-default-rfs7000-if-vlan44)#ip helper-address
172.16.10.3
RFController(config-profile-default-rfs7000-if-vlan44)#

RFController(config-profile-default-rfs7000-if-vlan1)#ip dhcp client request
options all
RFController(config-profile-default-rfs7000-if-vlan1)#
```

**no***interface vlan mode commands*

Negate a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [crypto|description|ip|shut-down|use]
```

**Parameters**

|                       |                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------|
| crypto                | Encryption module                                                                           |
| description           | Removes a VLAN description                                                                  |
| dhcp-relay-monitoring | Prohibits an on board DHCP server from responding to relayed DHCP packets on this interface |
| ip                    | Interface Internet Protocol config commands                                                 |
| shut-down             | Re-enables the selected interface                                                           |
| use                   | Defines the setting used with this command                                                  |

**Example**

```
RFController(config-profile-default-rfs7000-if-vlan44)#no use ip-access-list
in
RFController(config-profile-default-rfs7000-if-vlan44)#

RFController(config-profile-default-rfs7000-if-vlan44)#no allow-management
RFController(config-profile-default-rfs7000-if-vlan44)#
```

### *shutdown*

#### *interface vlan mode commands*

Shuts down the selected interface

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
shutdown
```

#### **Parameters**

None

#### **Example**

```
RFController(config-profile-default-rfs7000-if-vlan44)#shutdown  
RFController(config-profile-default-rfs7000-if-vlan44)#
```

**use****interface vlan mode commands**

Defines the settings used with this command

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

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

**Parameters**


---

|                                       |                                                                                                                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list in<br><IP-ACCESS-LIST> | Specifies the IP access list value <ul style="list-style-type: none"> <li>• in - Sets incoming packets</li> <li>• IP-ACCESS-LIST - Specifies the IP access list name</li> </ul> |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-profile-default-rfs7000-if-vlan44)#use ip-access-list in
test
% Error: ip_acl[test] does not exist
RFController(config-profile-default-rfs7000-if-vlan44)#
```

**NOTE**

The commands `clear`, `commit`, `end`, `exit`, `help`, `revert`, `show`, `service` are common across all chapters. For more information, see [Chapter 6, Common Commands](#).

---

### led

#### *profile commands*

Turns LEDs on/off on the access point

Supported in the following platforms:

- Mobility 7131 Series Access Point
- Mobility 650 Access Point

#### **Syntax**

```
led
```

#### **Parameters**

None

#### **Example**

```
RFController(config-profile-default-rfs7000)#led
% Error: led configuration not available for this platform
RFController(config-profile-default-rfs7000)#
```

## legacy-auto-downgrade

### *profile commands*

Enables device firmware to auto downgrade when legacy devices are detected

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
legacy-auto-downgrade
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default)#legacy-auto-downgrade  
RFController(config-profile-default)#
```

## legacy-auto-update

### *profile commands*

Enables a legacy device firmware to be auto updated

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
legacy-auto-update {BR650|BR7131} image <FILE NAME>
```

### Parameters

| legacy-auto-update          | Enables a legacy auto update                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [BR650 BR7131] image <FILE> | <ul style="list-style-type: none"> <li>• BR650 – Sets a legacy Mobility 650 Access Point update firmware image</li> <li>• BR7131 – Sets a legacy Mobility 7131 Series Access Point update firmware image               <ul style="list-style-type: none"> <li>• image – Sets the path to the image                   <ul style="list-style-type: none"> <li>• &lt;FILE&gt; – Specifies the path and filename, e.g. flash:/ap.img</li> </ul> </li> </ul> </li> </ul> |

### Example

```
RFController(config-profile-default-rfs7000)#legacy-auto-update BR650 image
flash:/ap47d.img
RFController(config-profile-default-rfs7000)#
RFController(config-profile-default-rfs7000)#legacy-auto-update
RFController(config-profile-default-rfs7000)#
```



## lldp

### *profile commands*

Configures *Link Layer Discovery Protocol* (lldp)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
lldp [holdtime <10-1800>|med-tlv-select|run|timer <5-900>]
lldp med-tlv-select [inventory-management|power-management]
```

### Parameters

|                                                           |                                                                                                                                                                                                                     |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| holdtime <10-1800>                                        | Sets the hold time value between <10-1800> in transmitted LLDP PDUs                                                                                                                                                 |
| med-tlv-select<br>[inventory-management power-management] | Media Endpoint Device TLVs <ul style="list-style-type: none"> <li>• inventory-management – Enables inventory management discovery</li> <li>• power-management – Enables extended power via MDI discovery</li> </ul> |
| run                                                       | Enables run link layer discovery protocol                                                                                                                                                                           |
| timer <5-900>                                             | Sets the timer for transmit interval between <5-900> seconds                                                                                                                                                        |

### Example

```
RFController(config-profile-default-rfs4000)#lldp timer 20
RFController(config-profile-default-rfs4000)#
```

## load-balancing

### *profile commands*

Configures load balancing parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
load-balancing
[ap-load-weightage|balance-ap-loads|balance-band-loads|balance-channel-loads|
band-ratio|client-weightage|equality-margin|hiwater-threshold|throughput-weightage]
load-balancing [ap-load-weightage|client-weightage|throughput-weightage]
[2.4ghz|5ghz] <0-100>
load-balancing balance-channel-loads [2.4ghz|5ghz]
load-balancing band-ratio 2.4ghz <0-10> 5ghz <0-10>
load-balancing equality-margin [2.4ghz|5ghz|ap|band] <0-100>
load-balancing hiwater-threshold[ap|channel-2.4ghz|channel-5ghz] <0-100> ]]
```

## Parameters

---

|                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ap-load-weightage<br> balance-ap-loads <br>balance-band-loads <br>balance-channel-loads <br>band-ratio client-weightage <br>equality-margin <br>hiwater-threshold <br>throughput-weightage] | <ul style="list-style-type: none"> <li>• ap-load-weightage [2.4ghz 5ghz] &lt;0-100&gt; – Configures weightage when calculating ap-load from radio loads</li> <li>• 2.4ghz – Weightage assigned to the 2.4ghz radio             <ul style="list-style-type: none"> <li>• 5ghz – Weightage assigned to the 5ghz radio                 <ul style="list-style-type: none"> <li>• &lt;0-100&gt; – Sets weightage as a percentage from 0 to 100</li> </ul> </li> </ul> </li> <li>• client-weightage [2.4ghz 5ghz] &lt;0-100&gt; – Configures weightage assigned to wireless client count</li> <li>• throughput-weightage [2.4ghz 5ghz] &lt;0-100&gt; – Configures weightage assigned to throughput             <ul style="list-style-type: none"> <li>• 2.4ghz – When calculating how much a 2.4GHz band/channel/radio is loaded</li> <li>• 5ghz – When calculating how much a 5GHz band/channel/radio is loaded                 <ul style="list-style-type: none"> <li>• &lt;0-100&gt; – Sets weightage as a percentage from 0 to 100</li> </ul> </li> </ul> </li> <li>• balance-channel-loads [2.4ghz 5ghz] – Enables balancing of channel loads amongst neighbors             <ul style="list-style-type: none"> <li>• 2.4ghz – Balance channel loads on 2.4ghz band</li> <li>• 5ghz – Balance channel loads on 5ghz band</li> </ul> </li> <li>• band-ratio 2.4ghz &lt;0-10&gt; 5ghz &lt;0-10&gt; – Configures relative loading of 2.4ghz and 5ghz bands             <ul style="list-style-type: none"> <li>• 2.4ghz – Relative loading of 2.4ghz</li> <li>• 5ghz – Relative loading of 5ghz                 <ul style="list-style-type: none"> <li>• &lt;0-10&gt; – Relative load in the ratio as a number between 0(no load) and 10</li> </ul> </li> </ul> </li> <li>• equality-margin [2.4ghz 5ghz ap band] &lt;0-100&gt; – Configures maximum load difference that can be considered equal             <ul style="list-style-type: none"> <li>• ap – When comparing loads on different APs</li> <li>• band – When comparing loads on different bands</li> <li>• 2.4ghz 5ghz] &lt;0-100&gt; – When comparing loads on different 2.4ghz and 5ghz channels                 <ul style="list-style-type: none"> <li>• &lt;0-100&gt; – Sets margin as a percentage of load between 1 and 100</li> </ul> </li> </ul> </li> <li>• hiwater-threshold[ap channel-2.4ghz channel-5ghz] &lt;0-100&gt; – Configures the load beyond which the load balancing kicks in             <ul style="list-style-type: none"> <li>• [ap – For the ap's total load</li> <li>• channel-2.4ghz – For the ap's channel on 2.4ghz</li> <li>• channel-5ghz – For the ap's channel on 5ghz</li> </ul> </li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Example

```

RFController(config-profile-default-rfs4000)#load-balancing
throughput-weightage 5 1
RFController(config-profile-default-rfs4000)#

RFController(config-profile-default-rfs4000)#load-balancing hiwater-threshold
ap 1
RFController(config-profile-default-rfs4000)#
RFController(config-profile-default-rfs4000)#load-balancing
balance-channel-loads 2.4ghz
RFController(config-profile-default-rfs4000)#

```

## local

### *profile commands*

Sets the username and password for local user authentication

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
local username <WORD> password <WORD>
```

### Parameters

- 
- |                                 |                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------|
| username <WORD> password <WORD> | • username <WORD> - Sets the username and password for local user authentication |
|                                 | • password <WORD> - A string of 8 to 21 characters                               |
- 

### Example

```
RFController(config-profile-default-rfs7000)#local username Denvor password  
admin123  
RFController(config-profile-default-rfs7000)#
```

## logging

### *profile commands*

Modifies message logging facilities

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
logging [aggregation-time <1-60>|buffered|console|facility|
forward|host||on|syslog]
logging [buffered|console|syslog] [<0-7>|alerts|
critical|debugging|emergencies|errors|informational|
notifications|warnings]
logging facility [local0|local1|local2|local3|
local4|local5|local6|local7]
logging host <IP>
logging forward on
```

## Parameters

|                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aggregation-time<br><1-60>                                                                         | Sets the number of seconds for aggregating repeated messages. The value can be configured between 1-60 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| buffered [<0-7> alerts critical debugging emergencies errors informational notifications warnings] | <p>Sets the buffered logging level</p> <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Enter the logging severity level (0-7)</li> <li>• alerts – Set the immediate action needed, (severity=1)</li> <li>• critical – Critical conditions, (severity=2)</li> <li>• debugging – Debugging messages, (severity=7)</li> <li>• emergencies – System is unusable, (severity=0)</li> <li>• errors – Error conditions, (severity=3)</li> <li>• informational – Informational messages, (severity=6)</li> <li>• notifications – Normal but significant conditions, (severity=5)</li> <li>• warnings – Warning conditions, (severity=4)</li> </ul> |
| console [<0-7> alerts critical debugging emergencies errors informational notifications warnings]  | Sets the console logging level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| forward on                                                                                         | <p>Forwards system debug messages to controller or cluster members</p> <ul style="list-style-type: none"> <li>• on – Enables forwarding debug messages</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| facility [local0 local1 local2 local3 local4 local5 local6 local7]                                 | <p>Syslog facility in which log messages are sent</p> <ul style="list-style-type: none"> <li>• local0 – Syslog facility local0</li> <li>• local1 – Syslog facility local1</li> <li>• local2 – Syslog facility local2</li> <li>• local3 – Syslog facility local3</li> <li>• local4 – Syslog facility local4</li> <li>• local5 – Syslog facility local5</li> <li>• local6 – Syslog facility local6</li> <li>• local7 – Syslog facility local7</li> </ul>                                                                                                                                                                                           |
| host <IP>                                                                                          | <p>Configures a remote host to receive log messages</p> <ul style="list-style-type: none"> <li>• &lt;IP&gt; – Remote host's IP address</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| on                                                                                                 | Enables the logging of system messages                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| syslog [<0-7> alerts critical debugging emergencies errors informational notifications warnings]   | Sets the syslog servers logging level                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Example

```
RFController(config-profile-default-rfs7000)#logging facility local4
RFController(config-profile-default-rfs7000)#logging monitor notifications
```

## mac-address-table

### *profile commands*

Configures the MAC address table

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mac-address-table [aging-time|static]
mac-address-table aging-time [0|<10-1000000>]
mac-address-table <MAC-Address> <WORD> [<WORD>|ge <1-4>|me1|pc <1-4>|vlan
<1-4094>]
```

### Parameters

|                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| aging-time [0 <10-1000000>]                                              | <p>Sets the duration a learned MAC address persists after the last update</p> <ul style="list-style-type: none"> <li>• 0 - Disables aging</li> <li>• &lt;10-1000000&gt; - Sets the aging time in seconds</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| static <MAC-Address> <WORD> [<WORD> ge <1-4> me1 pc <1-4> vlan <1-4094>] | <p>Static MAC address table entry</p> <ul style="list-style-type: none"> <li>• &lt;MAC-Address&gt; - Enter MAC address in AA-BB-CC-DD-EE-FF or AA:BB:CC:DD:EE:FF or AABB.CCDD.EEFF format <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies the VLAN name <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies the interface name</li> <li>• ge &lt;1-4&gt; - Specifies a GigabitEthernet interface value between 1 and 4</li> <li>• me1 - Specifies the FastEthernet interface</li> <li>• pc &lt;1-4&gt; - Specifies a Port-Channel interface value between 1 and 4</li> <li>• vlan &lt;1-4094&gt; - Specifies a VLAN index between 1 and 4094</li> </ul> </li> </ul> </li> </ul> |

### Example

```
RFController(config-profile-default-rfs7000)#mac-address-table static
00-40-96-B0-BA-2A vlan1 ge 1
RFController(config-profile-default-rfs7000)#
```

## mint

### *profile commands*

Configures MiNT protocol commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mint [dis||level|link|mlcp|spf-latency]
mint dispriority-adjustment <-255-255>
mint level [leve1|leve2] area-id <1-4294967295>
mint link [ip|listen|vlan]
mint link listen ip <A.B.C.D> {adjacency-hold-time <2-600>|cost
<1-10000>|hello-interval <1-120>|level [1|2]}
mint link [ip <A.B.C.D>|vlan <1-4095>] > {adjacency-hold-time <2-600>|cost
<1-10000>|hello-interval <1-120>|level [1|2]}
mint mlcp [12|13]
mint spf-latency <0-60>
```

### Parameters

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dis[priority-adjustment <-255-255> scatter] | <p>Sets the relative priority for the router to become DIS</p> <ul style="list-style-type: none"> <li>• priority-adjustment &lt;-255-255&gt; - Sets adjustment added to base priority <ul style="list-style-type: none"> <li>• &lt;-255-255&gt; - Priority adjustment value, added to fixed the base priority. Higher numbers result in higher priorities.</li> </ul> </li> </ul>                                                                                |
| level [leve1 leve2] area-id <1-4294967295>  | <p>Configures MiNT routing levels</p> <ul style="list-style-type: none"> <li>• leve1 - Configures local MiNT routing</li> <li>• leve2 - Configures inter-site MiNT routing</li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• area-id - Specifies a routing area identifier <ul style="list-style-type: none"> <li>• &lt;1-4294967295&gt; - Specifies an area identifier value</li> </ul> </li> </ul> |



---

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>link [ip &lt;A.B.C.D&gt; listen vlan &lt;1-4095&gt;] &lt;A.B.C.D&gt; {adjacency-hold-time &lt;2-600&gt; cost &lt;1-10000&gt; hello-interval &lt;1-120&gt; level [1 2]}</pre> | <p>Creates a MiNT routing link</p> <ul style="list-style-type: none"> <li>• ip &lt;A.B.C.D&gt; – Creates a MiNT tunnel over UDP/IP <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Specifies a peer IP address</li> </ul> </li> <li>• listen&lt;A.B.C.D&gt; – Creates listening link over UDP/IP <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Specifies a listening IP address</li> </ul> </li> <li>• vlan &lt;1-4095&gt; – Enables MiNT routing on a VLAN <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; – Specifies a VLAN index value</li> </ul> </li> </ul> <p>The following parameters are common for all the above:</p> <ul style="list-style-type: none"> <li>• adjacency-hold-time &lt;2-600&gt; – Adjacency lifetime after hello packets cease <ul style="list-style-type: none"> <li>• &lt;2-600&gt; – Specifies the lifetime in seconds</li> </ul> </li> <li>• cost &lt;1-10000&gt; – Specifies the link cost <ul style="list-style-type: none"> <li>• &lt;1-10000&gt; – Specifies the cost in arbitrary units</li> </ul> </li> <li>• hello-interval &lt;1-120&gt; – Hello packet interval <ul style="list-style-type: none"> <li>• &lt;1-120&gt; – Specifies the number of seconds between hello packets</li> </ul> </li> <li>• level[1 2] – Specifies existing routing levels <ul style="list-style-type: none"> <li>• 1 – Level 1 only (local)</li> <li>• 2 – Level 2 only (inter-site)</li> </ul> </li> </ul> |
| <pre>mlcp [I2 I3]</pre>                                                                                                                                                           | <p>Configures the MINT link creation protocol</p> <ul style="list-style-type: none"> <li>• I2 – MLCP over Layer 2 (VLAN) links</li> <li>• I3 – MLCP over Layer 3 (IP) links</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <pre>spf-latency &lt;0-60&gt;</pre>                                                                                                                                               | <p>Latency of SPF routing recalculation</p> <ul style="list-style-type: none"> <li>• &lt;0-60&gt; – Specifies the latency in seconds</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

---

### Example

```
RFController(config-profile-default-rfs7000)#mint level 1 area-id 88
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#mint link ip 1.2.3.4 level 1
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#show mint links
  vlan-1 : level 1, cost 10, 1 adjacencies, DIS 70.37.fa.be (self)
RFController(config-profile-default-rfs7000)#show mint stats
1 L1 neighbors
L1 LSP DB size 2 LSPs (1 KB)
2 L1 routes
Last SPF's took 0s
SPF (re)calculated 6 times.
levels 1
base priority 180
dis priority 180
RFController(config-profile-default-rfs7000)#show mint route
Destination : Next-Hop(s)
00.00.00.00 : 00.00.00.00
70.88.9e.c4 : 70.88.9E.C4
70.37.fa.be : 70.37.FA.BE
RFController(config-profile-default-rfs7000)#
```

## misconfiguration-recovery-time

### *profile commands*

Verifies controller connectivity after the configuration is received

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
misconfiguration-recovery-time <60-300>
```

### Parameters

---

|          |                                                   |
|----------|---------------------------------------------------|
| <60-300> | Sets the recovery time between 60 and 300 seconds |
|----------|---------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs7000)#misconfiguration-recovery-time  
65  
RFController(config-profile-default-rfs7000)#
```

## monitor

### *profile commands*

Enables critical resource monitoring

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
monitor <A.B.C.D> ping-mode [arp-icmp|arp-only vlan <1-4094>]
```

### Parameters

---

|                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>&lt;A.B.C.D&gt; ping-mode<br/>[arp-icmp arp-only vlan<br/>&lt;1-4094&gt;]</pre> | <p>Specify the critical resource IP address to be monitored</p> <ul style="list-style-type: none"> <li>• ping-mode [arp-icmp arp-only vlan &lt;1-4094&gt;] – Specify the protocol to be used to ping the critical resource <ul style="list-style-type: none"> <li>• arp-only – Uses either arp requests or icmp echo request to monitor critical resource (requires the AP/Controller to have an IP address)</li> <li>• arp-only vlan &lt;1-4094&gt; – Uses only probing arp requests to monitor critical resource (suitable for AP/Controller without IP address) <ul style="list-style-type: none"> <li>• vlan &lt;1-4094&gt; – Specify the VLAN on which the probing arp requests have to be sent</li> <li>• &lt;1-4094&gt; – Specify the VLAN ID</li> </ul> </li> </ul> </li> </ul> |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-critical-resource-policy-testpolicy)#monitor  
172.16.10.112 ping-mode arp-only vlan 1  
RFController(config-critical-resource-policy-testpolicy)#  
  
RFController(config-critical-resource-policy-testpolicy)#monitor  
172.16.10.112  
ping-mode arp-icmp  
RFController(config-critical-resource-policy-testpolicy)#  
  
RFController(config-critical-resource-policy-testpolicy)#show context  
critical-resource-policy testpolicy  
monitor 172.16.10.112 ping-mode arp-only vlan 1  
RFController(config-critical-resource-policy-testpolicy)#
```

## neighbor-inactivity-timeout

### *profile commands*

Configures neighbor inactivity timeout factor

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
neighbour-inactivity-timeout <1-1000>
```

### Parameters

---

<1-1000>

<1-1000> – Sets a timeout period, in seconds, for the neighbor-inactivity factor. The value can be anything between 1 to 1000 seconds

---

### Example

```
RFController(config-profile-default)#neighbor-inactivity-timeout 500  
RFController(config-profile-default)#
```

## neighbor-info-interval

### *profile commands*

Configures neighbor information exchange interval

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
neighbor-info-interval <1-100>
```

### Parameters

---

|         |                                                   |
|---------|---------------------------------------------------|
| <1-100> | Set interval in seconds as a number from 1 to 100 |
|---------|---------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs7000)#neighbor-info-interval 6  
RFController(config-profile-default-rfs7000)#
```

## no

### *profile commands*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [aaa|arp|autoinstall|ap-upgrade|automatic-write|bridge|cdp|
cluster|controller|controller-group|crypto|domain-lookup
|dscp-mapping|events|hb-holdtime|hb-interval|interface|ip|
legacy-auto-update|logging|local|mac-address-table|mint|name-server|
ntppreferred-controller-group|radius|rf-domain-manager|spanning-tree|use|
wep-shared-key-auth|service]
```

### Parameters

None

### Usage Guidelines

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

### Example

```
RFController(config-profile-default-rfs7000)#no cluster
RFController(config-profile-default-rfs7000)#
```

## noc

### *profile commands*

Configures the noc related settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
noc update-interval [<5-3600>|auto]
```

### Parameters

---

|                                    |                                                                                                                                                                                                                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| update-interval<br>[<5-3600> auto] | Configures the noc statistics update interval <ul style="list-style-type: none"><li>• &lt;5-3600&gt; - Specify the update interval between 5 and 3600 seconds</li><li>• auto - Noc statistics update interval is automatically adjusted by the Controller based on the load</li></ul> |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000)#noc update-interval 25  
RFController(config-profile-default-rfs4000)#
```



## ntp

### *profile commands*

Configure *Network Time Protocol* (NTP) values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ntp server <A.B.C.D> {autokey/key/prefer/version}
ntp server <A.B.C.D> autokey {prefer version <1-4>/version <1-4>}
ntp server <A.B.C.D> key md5 [0 <WORD>|2<WORD>|<WORD>]{prefer version
<1-4>/version <1-4>}
ntp server <A.B.C.D> prefer version <1-4>
ntp server <A.B.C.D> version <1-4> {prefer}
```

### Parameters

---

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server <A.B.C.D> | <p>Configures a NTP server</p> <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Configures an IP address for the server <ul style="list-style-type: none"> <li>• autokey {prefer version &lt;1-4&gt;  version &lt;1-4&gt;} – Configures an autokey peer authentication scheme</li> <li>• key md5 [0 &lt;WORD&gt; &lt;WORD&gt;  2 &lt;WORD&gt;] {prefer version &lt;1-4&gt;  version &lt;1-4&gt;} – Defines the authentication key for trusted time sources <ul style="list-style-type: none"> <li>• md5 [0 &lt;WORD&gt;  2 &lt;WORD&gt;  &lt;WORD&gt;] – Sets MD5 authentication <ul style="list-style-type: none"> <li>• 0 – Password is specified unencrypted</li> <li>• 2 – Password is specified encrypted with password encryption secret</li> <li>• &lt;WORD&gt; – Sets an authentication key</li> </ul> </li> <li>• prefer version &lt;1-4&gt; – Optional. Prefers this peer when possible.</li> <li>• version &lt;1-4&gt; {prefer} – Optional. Configures the NTP version</li> </ul> </li> </ul> </li> </ul> |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs7000)#ntp server 172.16.10.10
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#ntp server 172.16.10.1 version 1
prefer
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#ntp server 172.16.10.9 key md5 0
sharedkey1 prefer version 1
RFController(config-profile-default-rfs7000)#
```

## preferred-controller-group

### *profile commands*

Specifies the controller group the system prefers for adoption

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
preferred-controller-group <WORD>
```

### Parameters

---

|        |                                                                     |
|--------|---------------------------------------------------------------------|
| <WORD> | Specifies the controller group name the system prefers for adoption |
|--------|---------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs7000)#preferred-controller-group  
testgroup1  
RFController(config-profile-default-rfs7000)#
```

## power-config

### *profile commands*

Configures the power mode feature

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
power-config [af-option|at-option|mode]
power-config af-option[range|throughput]
power-config at-option [range|throughput]
power-config mode [auto|3af]
```

### Parameters

|                              |                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| af-option [range throughput] | Configures the af power option mode <ul style="list-style-type: none"> <li>• range – Configures the af power range mode</li> <li>• throughput – Configures the power throughput mode</li> </ul> |
| at-option [range throughput] | Configures the af power option mode <ul style="list-style-type: none"> <li>• range – Configures the af power range mode</li> <li>• throughput – Configures the power throughput mode</li> </ul> |
| mode [auto 3af]              | Configures the power mode of this AP <ul style="list-style-type: none"> <li>• 3af – Forces an AP bring up at the 3af power mode</li> <li>• auto – Power the detection auto mode</li> </ul>      |

### Example

```
RFController(config-profile-defalut-rfs7000)#power-config af-option range
% Warning: AP must be restarted for power-management change to take effect.
RFController(config-profile-defalut-rfs7000)#
RFController(config-profile-defalut-rfs7000)#power-config at-option
throughput

% Warning: AP must be restarted for power-management change to take effect.
RFController(config-profile-defalut-rfs7000)#
```

## radius

### *profile commands*

Configures device-level RADIUS authentication parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
radius [nas-identifier|nas-port-id] <WORD>
```

### Parameters

|                       |                                                                                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| nas-identifier <WORD> | Specifies the RADIUS NAS Identifier attribute used by a device <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies the NAS identifier</li> </ul> |
| nas-port-id<WORD>     | Specifies the RADIUS NAS port ID attribute tused by a device <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies the NAS port ID</li> </ul>      |

### Example

```
RFController(config-profile-default-rfs7000)#radius nas-port-id 1
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#radius nas-identifier test
RFController(config-profile-default-rfs7000)#
```

## rf-domain-manager

### *profile commands*

Enables the RF Domain manager feature

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
rf-domain-manager [capable|priority <1-10000>]
```

### Parameters

|                    |                                                                                                                                                   |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| capable            | Enables a device to become site manager                                                                                                           |
| priority <1-10000> | Assigns a priority value for site manager selection <ul style="list-style-type: none"> <li>• &lt;1-10000&gt; - Select a priority value</li> </ul> |

### Example

```
RFController(config-profile-default-rfs7000)#rf-domain-manager priority 9
RFController(config-profile-default-rfs7000)#
```

```
RFController(config-profile-default-rfs7000)#rf-domain-manager capable
RFController(config-profile-default-rfs7000)#
```

## service

### *profile commands*

Service Commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
service [watchdog|show cli]
```

### Parameters

---

|                     |                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| [watchdog show cli] | <ul style="list-style-type: none"><li>• watchdog – Enables the watchdog</li><li>• show cli – Displays running system information</li></ul> |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs7000)#service watchdog  
RFController(config-profile-default-rfs7000)#
```

## spanning-tree

### *profile commands*

Enables spanning tree commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
spanning-tree [errdisable|mst|portfast]
spanning-tree errdisable recovery [cause bpduguard|interval
<10-1000000>]
spanning-tree mst [<0-15> priority <0-61440>| cisco-interopability
[enable|disable] |enable|forward-time <4-30> |hello-time
<1-10>|instance <1-15>|max-age <4-60> |max-hops <7-127>|region
<LINE>|revision <0-255>]
spanning-tree portfast [bpdufilter| bpduguard] default
```

## Parameters

|                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| errdisable recovery [cause<br>bpduguard  interval<br><10-1000000>]                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Disables error</li> <li>recovery – Enables the timeout mechanism for a port to be recovered</li> <li>cause bpduguard – Specifies the reason for errdisable</li> <li>bpduguard – Recovers from errdisable due to bpduguard</li> <li>interval &lt;10-1000000&gt; – Specifies the interval after which a port is enabled</li> <li>&lt;10-1000000&gt; – Specifies an errdisable-timeout interval in seconds.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| mst [<0-15> priority<br><0-61440>   cisco-interopability<br>[enable disable]  enable  <br>forward-time <4-30>  hello-time<br><1-10>  instance<br><1-15>  max-age <4-60>  <br>max-hops <7-127>  region<br><LINE>  revision <0-255>] | <p>Configures multiple spanning tree commands</p> <ul style="list-style-type: none"> <li>&lt;0-15&gt; – Specifies the number of instances required for configuration <ul style="list-style-type: none"> <li>priority &lt;0-61440&gt; – Sets the bridge priority for an instance to the value specified. Use the no parameter with this command to restore the default bridge priority value <ul style="list-style-type: none"> <li>&lt;0-61440&gt; – Bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root)</li> </ul> </li> </ul> </li> <li>cisco-interopability [enable disable] – Enables/disables CISCO interoperability</li> <li>Enable – Enables the multiple spanning tree protocol</li> <li>forward-time &lt;4-30&gt; – Specifies the forwarding delay time in seconds between 4 -30</li> <li>hello-time &lt;1-10&gt; – Specifies the hello BPDU interval in seconds within the range 1-10</li> <li>Instance &lt;1-15&gt; – Defines the instance ID to which the VLAN is associated</li> <li>max-age &lt;4-60&gt; – Maximum time to listen for the root bridge in seconds. Enter a value between 4 and 60</li> <li>max-hop &lt;7-127&gt; – Maximum hops when BPDU is valid</li> <li>region &lt;LINE&gt; – MST region</li> <li>revision &lt;0-255&gt; – Sets the revision number of the MST bridge. <ul style="list-style-type: none"> <li>&lt;0-255&gt; – Defines the revision number for configuration information</li> </ul> </li> </ul> |
| portfast [bpdufilter  bpduguard]<br>default                                                                                                                                                                                        | <p>Enables the portfast feature on a bridge</p> <ul style="list-style-type: none"> <li>bpdufilter default – Use the bpd-filter command to set the BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to the default value.<br/>The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFast enabled ports do not transmit or receive BPDUs</li> <li>bpduguard default – Guards portfast ports against BPDU receive <ul style="list-style-type: none"> <li>default – Enables the BPDU filter on portfast enabled ports by default</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Usage Guidelines

If a bridge does not hear bridge protocol data units (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, 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 works based on instances. An instance is a group of VLANs with a common spanning tree. A single VLAN cannot be associated with multiple instances.



Controllers with the same instance, VLAN mapping, revision number and region names define a unique region. Controllers in the same region exchange bridge protocol data units (BPDUs) with instance record information within.

**Example**

```
RFController(config-profile-defaulttrfs7000)#spanning-tree errdisable recovery
cause bpduguard
RFController(config-profile-defaulttrfs7000)#
RFController(config-profile-defaulttrfs7000)#spanning-tree mst 1 priority 4096
RFController(config-profile-defaulttrfs7000)#
RFController(config-profile-defaulttrfs7000)#spanning-tree portfast bpdufilter
default
RFController(config-profile-defaulttrfs7000)#
```

## USE

### *profile commands*

Defines the settings used with this command

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax Profiles**

```
use [adoption-policy|advanced-wips-policy|bridging-policy|  
captive-portal|critical-resource-policy|dhcp-server-policy|event-system-poli  
cy|firewall-policy|igmp-snoop-policy|management-policy|  
radius-server-policy|role-policy]
```

### **Syntax Device Mode**

```
use [adoption-policy|advanced-wips-policy|bridging-policy|  
captive-portal|critical-resource-policy|dhcp-server-policy|  
firewall-policy|igmp-snoop-policy|management-policy|profile|  
radius-server-policy|rf-domain|role-policy|  
smart-rf-policy|trustpoint|wips-policy]
```

---

### **NOTE**

The Parameter Table contains the 'use' command parameters for the Profiles and Device modes.

---

## Parameters

---

|                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| use [adoption-policy   advanced-wips-policy   bridging-policy   captive-portal   critical-resource-policy   dhcp-server-policy   firewall-policy   igmp-snoop-policy   management-policy   profile   radius-server-policy   rf-domain   role-policy   smart-rf-policy   trustpoint   wips-policy] | <p>Uses the policies as defined</p> <ul style="list-style-type: none"> <li>• adoption-policy – Sets an adoption policy</li> <li>• advanced-wips-policy – Creates/configures an advanced-wips policy</li> <li>• bridging-policy – Sets the bridging policy</li> <li>• captive-portal – Captive portal access configuration</li> <li>• critical-resource-policy – Sets a critical resource policy</li> <li>• dhcp-server-policy – Sets a DHCP server policy</li> <li>• event-system-policy – Sets an event system policy</li> <li>• firewall-policy – Sets the firewall policy</li> <li>• igmp-snoop-policy – Sets an IGMP snoop policy</li> <li>• management-policy – Sets a management policy</li> <li>• radius-server-policy – Sets a device's onboard RADIUS policy</li> <li>• rf-domain – Specify the RF-Domain from which the connected device receives its configuration</li> <li>• role-policy – Sets a role policy configuration</li> <li>• smart-rf-policy – Configures the smart-rf policy</li> <li>• trustpoint &lt;WORD&gt; – Uses a trustpoint for the service</li> <li>• https – Uses the trustpoint for HTTPS <ul style="list-style-type: none"> <li>• radius-ca-certificate – Uses the trustpoint as a certificate authority, for validating client certificates using EAP</li> <li>• radius-server-certificate – Uses the trustpoint for a RADIUS server certificate</li> </ul> </li> <li>• wips-policy – Configures the WIPS policy</li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Example

```

RFController(config-profile-default-rfs7000)#use role-policy test
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#use adoption-policy test
RFController(config-profile-default-rfs7000)#

RFController(config-device-00-15-70-37-FA-BE)#use trustpoint trust1 https
radius-ca-certificate radius-server-certificate
RFController(config-device-00-15-70-37-FA-BE)#

```

## vpn

### *profile commands*

Configures VPN settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
vpn authentication-method [local|radius]
```

### Parameters

---

|                                         |                                                                                                                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication-method<br>[local radius] | Selects an authentication scheme <ul style="list-style-type: none"><li>• local - Used for user based authentication</li><li>• radius - Used for RADIUS server authentication</li></ul> |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Usage Guidelines

*Virtual Private Network* (VPN) enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt information at the IP level.

### Example

```
RFController(config-profile-default-rfs7000)#vpn authentication-method local
RFController(config-profile-default-rfs7000)#

RFController(config-profile-default-rfs7000)#vpn authentication-method
radius
RFController(config-profile-default-rfs7000)#
```

## wep-shared-key-auth

### *profile commands*

Enables support for 802.11 WEP shared key authentication

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
wep-shared-key-auth
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default-rfs7000)#wep-shared-key-auth  
RFController(config-profile-default-rfs7000)#
```

## Device specific commands

Use the (config) instance to configure device specific parameters.

To navigate to this instance, use the following commands:

```
RFController(config)#br7131?
RFController(config)#br7131 00-15-70-88-9E-C4
RFController(config-device-00-15-70-88-9E-C4)
```

Table 23 Summarizes device mode commands

**TABLE 23** device mode commands

| Command                                | Description                                                             | Reference                |
|----------------------------------------|-------------------------------------------------------------------------|--------------------------|
| <a href="#">ap-upgrade</a>             | Upgrades AP firmware                                                    | <a href="#">page 525</a> |
| <a href="#">area</a>                   | Sets the name of area where the system is located                       | <a href="#">page 526</a> |
| <a href="#">contact</a>                | Sets contact information                                                | <a href="#">page 527</a> |
| <a href="#">country-code</a>           | Configures the controller country code                                  | <a href="#">page 528</a> |
| <a href="#">dhcp-redundancy</a>        | Enables DHCP redundancy                                                 | <a href="#">page 529</a> |
| <a href="#">floor</a>                  | Sets the name of a floor within a building where the system is deployed | <a href="#">page 530</a> |
| <a href="#">hostname</a>               | Sets a system's network name                                            | <a href="#">page 531</a> |
| <a href="#">layout-coordinates</a>     | Configures layout coordinates                                           | <a href="#">page 532</a> |
| <a href="#">location</a>               | Configures the location the system is deployed                          | <a href="#">page 533</a> |
| <a href="#">mac-name</a>               | Configures MAC name to name mappings                                    | <a href="#">page 534</a> |
| <a href="#">neighbor-info-interval</a> | Configures the neighbor information exchange interval                   | <a href="#">page 535</a> |
| <a href="#">override-wlan</a>          | Configures RF Domain level overrides for a WLAN                         | <a href="#">page 536</a> |
| <a href="#">remove-override</a>        | Removes overrides from a device                                         | <a href="#">page 537</a> |
| <a href="#">rsa-key</a>                | Assigns a RSA key to SSH                                                | <a href="#">page 538</a> |
| <a href="#">sensor-server</a>          | Configures a Brocade AirDefense sensor server                           | <a href="#">page 539</a> |
| <a href="#">stats</a>                  | Configures statistics settings                                          | <a href="#">page 540</a> |
| <a href="#">timezone</a>               | Configures controller timezone settings                                 | <a href="#">page 541</a> |
| <a href="#">trustpoint</a>             | Assigns a trustpoint to a service                                       | <a href="#">page 542</a> |
| <a href="#">wwan</a>                   | Configures wireless WAN parameters                                      | <a href="#">page 543</a> |

## ap-upgrade

### *device mode commands*

Upgrades access point firmware to the latest version

Supported in the following platforms:

- Mobility 7131 Series Access Point
- Mobility 650 Access Point

### **Syntax**

```
ap-upgrade [all|br650|br7131]
ap-upgrade [br650|br7131] <MAC>
```

### **Parameters**

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [all br650 br7131] | <ul style="list-style-type: none"><li>• all - Upgrades all access points</li><li>• br650 &lt;MAC&gt; - Upgrades an BR650 device<ul style="list-style-type: none"><li>• DEVICE-BR650 - MAC address of a BR650 device</li></ul></li><li>• br7131 - Upgrades a Mobility 7131 Series Access Point<ul style="list-style-type: none"><li>• DEVICE-BR7131 - MAC address of a Mobility 7131 Series Access Point</li></ul></li></ul> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-device-00-15-70-37-FA-BE)#ap-upgrade all
RFController(config-device-00-15-70-37-FA-BE)#
```

### area

#### *device mode commands*

Sets the name of area where the system is located

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
area <WORD>
```

#### **Parameters**

---

|             |                                                   |
|-------------|---------------------------------------------------|
| area <WORD> | Sets the name of area where the system is located |
|-------------|---------------------------------------------------|

---

#### **Example**

```
RFController(config-device-00-15-70-37-FA-BE)#area RMZEcoSpace
RFController(config-device-00-15-70-37-FA-BE)#
```



## contact

### *device mode commands*

Defines a contact for a deployed devices

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
contact <WORD>
```

### Parameters

---

|                |                                    |
|----------------|------------------------------------|
| contact <WORD> | Enter a name to define the contact |
|----------------|------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-88-9E-C4)#contact brocade
RFController(config-device-00-15-70-88-9E-C4)#
```

## country-code

### *device mode commands*

Sets the country of operation. All existing radio configurations are erased.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
country-code <WORD>
```

### Parameters

---

|                     |                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| country-code <WORD> | Configures the device to operate in a defined country. <country-code> is the 2 letter ISO-3166 country code |
|---------------------|-------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-88-9E-C4)#country-code us
RFController(config-device-00-15-70-88-9E-C4)#
```

## dhcp-redundancy

### *device mode commands*

Enables DHCP redundancy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dhcp-redundancy
```

### **Parameters**

None

### **Example**

```
RFController(config-device-00-15-70-88-9E-C4)#dhcp-redundancy  
RFController(config-device-00-15-70-88-9E-C4)#
```

### floor

#### *device mode commands*

Sets the name of a floor within a building where the system is located

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Syntax**

```
floor <WORD>
```

#### **Parameters**

---

|        |                                                                        |
|--------|------------------------------------------------------------------------|
| <WORD> | Sets the name of a floor within a building where the system is located |
|--------|------------------------------------------------------------------------|

---

#### **Example**

```
RFController(config-device-00-15-70-37-FA-BE)#floor 5floor  
RFController(config-device-00-15-70-37-FA-BE)#
```

## hostname

### *device mode commands*

Sets system's network name

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
hostname <WORD>
```

### **Parameters**

---

|                 |                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| hostname <WORD> | Sets the name of the controller. This name is displayed when the controller is accessed from any network. |
|-----------------|-----------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-device-00-15-70-88-9E-C4)#hostname myrfs7000
```

## layout-coordinates

### *device mode commands*

Configures layout coordinates for the device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
layout-coordinates <0.0-4096.0> <0.0-4096.0>
```

### Parameters

- 
- |              |              |                                                            |
|--------------|--------------|------------------------------------------------------------|
| <0.0-4096.0> | <0.0-4096.0> | • <0.0-4096.0> - Specify X coordinate between 0 and 4096.0 |
|              |              | • <0.0-4096.0> - Specify Y coordinate between 0 and 4096.0 |
- 

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#layout-coordinates 1.5 2
RFController(config-device-00-15-70-37-FA-BE)#

RFController(config-device-00-15-70-37-FA-BE)#show context
rfs7000 00-15-70-37-FA-BE
  use profile Profile_7K_TechPubs
  use rf-domain RFDOMAIN_TechPubs
  hostname RFController
  layout-coordinates 1.5 2.0
  license AP
8088bb045018988b85bc057b560ab7edbc68029885fbcc680a96194dfbeedc28d4117058eb53b
d8b
  license AAP
8088bb045018988b5985f7127ca1d354bc68029885fbcc68b6025fb695384946d4117058eb53b
d8b
  autoinstall configuration
  autoinstall firmware
  use dhcp-server-policy DHCP_POLICY_TechPubs
  logging on
  logging console warnings
  logging buffered warnings
RFController(config-device-00-15-70-37-FA-BE)#
```

## location

### *device mode commands*

Configures the location where a controller managed device is deployed

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
location <WORD>
```

### Parameters

---

|        |                                                                        |
|--------|------------------------------------------------------------------------|
| <WORD> | Configures the location where the device is deployed within a building |
|--------|------------------------------------------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#location SarjapurRingRoad
RFController(config-device-00-15-70-37-FA-BE)#show context
rfs7000 00-15-70-37-FA-BE
  use profile default-rfs7000
  use rf-domain default
  hostname RFController
  building RMZEcospace
  floor 5floor
  location SarjapurRingRoad
```

## mac-name

### *device mode commands*

Configures a MAC name for mappings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mac-name <AA-BB-CC-DD-EE-FF> <WORD>
```

### Parameters

---

|                                        |                                                                                                                                                                  |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;AA-BB-CC-DD-EE-FF&gt;</code> | Configures a MAC address                                                                                                                                         |
| <code>&lt;WORD&gt;</code>              | <ul style="list-style-type: none"> <li>• <code>&lt;WORD&gt;</code> - Specifies the 'friendly' name used for this MAC address in events and statistics</li> </ul> |

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#mac-name 11-22-33-44-55-66
testrfs7000
RFController(config-device-00-15-70-37-FA-BE)#commit
RFController(config-device-00-15-70-37-FA-BE)#show context

rfs7000 00-15-70-37-FA-BE
  use profile default-rfs7000
  use rf-domain default
  hostname RFController
  mac-name 11-22-33-44-55-66 testrfs7000
  interface me1
  interface ge1
    switchport mode access
    switchport access vlan 1
  interface ge2
  interface ge3
  interface ge4
  interface vlan1
    ip address 172.16.10.2/24
RFController(config-device-00-15-70-37-FA-BE)#
```



## neighbor-info-interval

### *device mode commands*

Configures the neighbor information exchange interval

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
neighbor-info-interval <1-100>
```

### Parameters

---

|                                   |                                                                          |
|-----------------------------------|--------------------------------------------------------------------------|
| neighbor-info-interval<br><1-100> | Sets the neighbor information exchange interval between 1 to 100 seconds |
|-----------------------------------|--------------------------------------------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#neighbor-info-interval 10  
RFController(config-device-00-15-70-37-FA-BE)#
```

## override-wlan

### *device mode commands*

Configures RF Domain level overrides for a WLAN

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
override-wlan WLAN [ssid <WORD>|vlan-pool <1-4094> {limit} <0-8192>|
wpa-wpa2-psk <WORD>]
```

### Parameters

---

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WLAN [ssid <WORD> vlan-pool <1-4094> wpa-wpa2-psk <WORD>] | Enter the name of the WLAN to be configured                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                                           | <ul style="list-style-type: none"> <li>• ssid &lt;WORD&gt; - Configures the SSID for this WLAN <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specifies a case-sensitive alphanumeric SSID</li> </ul> </li> <li>• vlan-pool &lt;1-4094&gt; {limit} - Configures a pool of VLANs for the WLAN <ul style="list-style-type: none"> <li>• &lt;1-4094&gt; - Specifies a VLAN ID between 1 and 4094 <ul style="list-style-type: none"> <li>• {limit &lt;0-8192&gt;} - Specifies a value between 0 and 8192 to limit the number of users on this VLAN</li> </ul> </li> </ul> </li> <li>• wpa-wpa2-psk &lt;WORD&gt; - Configures the WPA-WPA2 key or passphrase for the WLAN</li> </ul> |

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#override-wlan test vlan-pool 8
limit 9
RFController(config-device-00-15-70-37-FA-BE)#commit
RFController(config-device-00-15-70-37-FA-BE)#show context

rfs7000 00-15-70-37-FA-BE
  use profile default-rfs7000
  use rf-domain default
  hostname RFController
  override-wlan test vlan-pool 8 limit 9
  mac-name 11-22-33-44-55-66 testrfs7000
  interface me1
  interface ge1
    switchport mode access
    switchport access vlan 1
  interface ge2
  interface ge3
  interface ge4
  interface vlan1
    ip address 172.16.10.2/24
RFController(config-device-00-15-70-37-FA-BE)#
```

## remove-override

### *device mode commands*

Removes overrides from a device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
remove-override <parameters>
```

### Parameters

None

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#remove-override ?
  all                Remove all overrides for the device
  arp                Static Address Resolution Protocol (ARP)
  autoinstall        Autoinstall Configuration commands
  bridge             Bridge group commands
  cluster            Cluster configuration
  contact            The contact
  country-code       The country of operation
  dhcp-redundancy    DHCP redundancy
  domain-lookup      Domain lookup
  dscp-mapping        IP DSCP to 802.1p priority mapping for untagged frames
  events             System event messages
  firewall           Enable/Disable firewall
  global             Remove global overrides for the device but keeps
                    per-interface overrides
  hb-holdtime        Hold time
  hb-interval        Heartbeat interval
  interface          Select an interface to configure
  ip                 Internet Protocol (IP)
  location           The location
                    Modify message logging facilities
  mac-address-table MAC Address Table
  name-server        Name server
  ntp                Configure NTP
  override-wlan      Overrides for wlans
  power-config       Configure power mode
  rf-domain-manager  RF Domain Manager
  sensor-server      Brocade AirDefense WIPS sensor server configuration
  timezone           The timezone
  use                Set setting to use
  service            Service Commands
```

## rsa-key

### *device mode commands*

Assigns a RSA key to a service

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
rsa-key ssh <WORD>
```

### Parameters

---

ssh <WORD>

Assigns the RSA key to SSH

- <WORD> – Specifies the RSA key name. This should be installed on the device using PKI commands in enable mode
- 

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#rsa-key ssh rsa-key1
RFController(config-device-00-15-70-37-FA-BE)#
```

## sensor-server

### *device mode commands*

Configures a Brocade AirDefense sensor server

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
sensor-server <1-3> ip <A.B.C.D> {port} [443|8443|<1-65535>]
```

### Parameters

---

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>&lt;1-3&gt; ip &lt;A.B.C.D&gt; {port} &lt;1-65535&gt;</pre> | <pre>&lt;1-3&gt; - Select a server to configure with an IP address and optional port number • ip &lt;A.B.C.D&gt; - Configures the IP address of the server • {port} [443 8443 &lt;1-65535&gt;] - Specifies port value • 443 - The default port used by AirDefense Server • 8443 - The default port used by Advanced-WIPS on a controller • &lt;1-65535&gt; - Manually sets the port number of the Advanced-WIPS/AirDefense server</pre> |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#sensor-server 2 ip 172.16.10.7
port 1080
RFController(config-device-00-15-70-37-FA-BE)#

RFController(config-device-00-15-70-37-FA-BE)#show context
rfs7000 00-15-70-37-FA-BE
use profile default-rfs7000
use rf-domain default
hostname RFController
timezone india
sensor-server 2 ip 172.16.10.7 port 1080
interface me1
interface ge1
switchport mode access
switchport access vlan 1
interface ge2
interface ge3
interface ge4
interface vlan1
ip address 172.16.10.2/24
interface vlan4
ip address 157.235.208.252/24
RFController(config-device-00-15-70-37-FA-BE)#
```

## stats

### *device mode commands*

Configures the statistics related settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
stats open-window <1-2> {sample-interval <5-86640>} {size <3-100>}
```

### Parameters

---

|                                                              |                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| open-window <1-2> {sample-interval <5-86640>} {size <3-100>} | Opens a stats-window to fetch trending data. Set the index value between 1 and 2 <ul style="list-style-type: none"><li>• {sample-interval &lt;5-86640&gt;} - Sets the sample interval value between 5 and 86640 seconds</li><li>• {size &lt;3-100&gt;} - Sets the stats window size and number of samples collected</li></ul> |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#stats open-window 1
sample-interval 77 size 10
RFController(config-device-00-15-70-37-FA-BE)#
```

## timezone

### *device mode commands*

Configures controller timezone settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
timezone <timezone>
```

### **Parameters**

---

|                     |                                             |
|---------------------|---------------------------------------------|
| timezone <timezone> | Configures the controller timezone settings |
|---------------------|---------------------------------------------|

---

### **Example**

```
RFController(config-device-00-15-70-37-FA-BE)#timezone sanjose
RFController(config-device-00-15-70-37-FA-BE)#
```

## trustpoint

### *device mode commands*

Assigns a trustpoint to a service

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
trustpoint [https|radius-ca|radius-server] <WORD>
```

### Parameters

- 
- |                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [https radius-ca radius-server]<br><WORD> | <ul style="list-style-type: none"><li>• https &lt;WORD&gt; - Assigns the trustpoint to HTTPS</li><li>• radius-ca &lt;WORD&gt; - Assigns the trustpoint as a certificate authority for validating client certificates using EAP</li><li>• radius-server &lt;WORD&gt; - Assigns the trustpoint for a RADIUS server certificate<ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specifies the trustpoint name. This should be installed on the device using PKI commands in enable mode</li></ul></li></ul> |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

### Example

```
RFController(config-device-00-15-70-37-FA-BE)#trustpoint radius-ca trust2  
RFController(config-device-00-15-70-37-FA-BE)#
```



## wwan

### *device mode commands*

Configures Wireless WAN interface parameters

Supported in the following platforms:

- Mobility RFS4000 Controller
- Mobility RFS6000 Controller

### Syntax

```
wwan [apn <WORD>|auth-type|crypto-map <CRYPTO-MAP>|enable|ip
|password|username <WORD>]
wwan auth-type [chap|mschap|mschap-v2|pap]
wwan ip nat [inside|outside]
wwan password [2|<WORD>]
```

### Parameters

|                                       |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| apn <WORD>                            | Enter the access point name provided by the service provider <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – A string of up to 25 characters</li> </ul>                                                                                                                                                                                                |
| auth-type [chap mschap mschap-v2 pap] | Specify the authentication-type from the following: <ul style="list-style-type: none"> <li>• chap – Challenge Handshake Authentication Protocol</li> <li>• mschap – Microsoft CHAP extensions</li> <li>• mschap-v2 – Microsoft CHAP extensions Version 2</li> <li>• pap – Password Authentication Protocol</li> </ul>                                          |
| crypto-map <CRYPTO-MAP>               | Enter a crypto map for wireless WAN <ul style="list-style-type: none"> <li>• &lt;CRYPTO-MAP&gt; – A string of up to 256 characters</li> </ul>                                                                                                                                                                                                                  |
| enable                                | Enable wireless WAN feature                                                                                                                                                                                                                                                                                                                                    |
| ip nat [inside outside]               | Configures Internet Protocol (IP) settings <ul style="list-style-type: none"> <li>• nat [inside outside] – Specifies <i>Network Address Translation</i> (NAT) information <ul style="list-style-type: none"> <li>• inside – Marks wireless WAN as NAT inside interface</li> <li>• outside – Marks wireless WAN as NAT outside interface</li> </ul> </li> </ul> |
| username <WORD>                       | Enter the username provided by the service provider <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – A string of up to 32 characters</li> </ul>                                                                                                                                                                                                         |
| password <WORD>                       | Enter the password provided by the service provider <ul style="list-style-type: none"> <li>• 2 – Enter encrypted password</li> <li>• &lt;WORD&gt; – A string of up to 30 characters</li> </ul>                                                                                                                                                                 |

### Example

```
RFController(config-device-00-23-68-88-0D-A7)#wwan enable
RFController(config-device-00-23-68-88-0D-A7)#

RFController(config-device-00-23-68-88-0D-A7)#wwan username testuser
RFController(config-device-00-23-68-88-0D-A7)#

RFController(config-device-00-23-68-88-0D-A7)#wwan password brocadetest
RFController(config-device-00-23-68-88-0D-A7)#
```

## 8 Device specific commands

# aaa-policy

---

## In this chapter

- [aaa-policy](#) ..... 546

This chapter summarizes the aaa-policy commands within the CLI structure.

Use the (config) instance to configure aaa-policy related configuration commands. To navigate to the config-aaa-policy instance, use the following commands:

```

RFController(config)#aaa-policy <policy-name>
RFController(config)#aaa-policy test
RFController(config-aaa-policy-test)#?
AAA Policy Mode commands:
  accounting          Configure accounting parameters
  authentication      Configure authentication 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
  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

RFController(config-aaa-policy-test)#

```

## aaa-policy

Table 24 Summarizes aaa-policy commands

**TABLE 24** aaa-policy Commands

| Command                             | Description                                                                                          | Reference                |
|-------------------------------------|------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">accounting</a>          | Configures accounting parameters                                                                     | <a href="#">page 547</a> |
| <a href="#">authentication</a>      | Configures authentication parameters                                                                 | <a href="#">page 551</a> |
| <a href="#">clrscr</a>              | Clears the display screen                                                                            | <a href="#">page 559</a> |
| <a href="#">commit</a>              | Commits (saves) the changes made in the current session                                              | <a href="#">page 562</a> |
| <a href="#">do</a>                  | Runs commands from EXEC mode                                                                         | <a href="#">page 563</a> |
| <a href="#">end</a>                 | Ends and exits the current mode and moves to the PRIV EXEC mode                                      | <a href="#">page 565</a> |
| <a href="#">exit</a>                | Ends the current mode and moves to the previous mode                                                 | <a href="#">page 566</a> |
| <a href="#">health-check</a>        | Configures health check parameters                                                                   | <a href="#">page 566</a> |
| <a href="#">help</a>                | Displays the interactive help system                                                                 | <a href="#">page 568</a> |
| <a href="#">mac-address-format</a>  | Configures the format the MAC-addresses must be filled                                               | <a href="#">page 555</a> |
| <a href="#">no</a>                  | Negates a command or sets its default                                                                | <a href="#">page 556</a> |
| <a href="#">revert</a>              | Reverts the changes to their last saved configuration                                                | <a href="#">page 569</a> |
| <a href="#">server-pooling-mode</a> | Defines the method for selecting a server from the pool of configured AAA servers                    | <a href="#">page 557</a> |
| <a href="#">service</a>             | Invokes service commands to troubleshoot or debug ( <code>config-if</code> ) instance configurations | <a href="#">page 570</a> |
| <a href="#">show</a>                | Displays running system information                                                                  | <a href="#">show</a>     |
| <a href="#">use</a>                 | Defines the settings used for AAA commands                                                           | <a href="#">page 558</a> |
| <a href="#">write</a>               | Writes information to memory or terminal                                                             | <a href="#">page 559</a> |

## accounting

### *aaa-policy*

Configures accounting parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

accounting [interim|server|type]
accounting interim interval <60-3600>

accounting server [<1-6>|preference]
accounting server <1-6> [dscp <0-63>|host |nai-routing|onboard|
proxy-mode|retry-timeout-factor <50-200>|timeout]
accounting server <1-6> host <WORD> secret [0 <WORD>|2 <WORD>|<WORD>] {port}
<1-65535>
accounting server <1-6> nai-routing realm-type [prefix|suffix] realm <WORD>
{strip}
accounting server <1-6> onboard [self|controller]
accounting server <1-6> proxy-mode [none|through-controller|
through-rf-domain-manager]
accounting server <1-6> timeout <1-30060> {attempts} <1-100>

accounting server preference [auth-server-host|auth-server-number|none

accounting type [start-interim-stop|start-stop|stop-only]]

```

**Parameters**

|                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interim interval <60-3600>                                                                                                                                  | <p>Configures interim accounting parameters</p> <ul style="list-style-type: none"> <li>interval &lt;60-3600&gt; – Configures the interval (in seconds) after which interim-accounting updates are sent</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| server [<1-6> [dscp <0-63>   host <WORD> secret <WORD> {port}   nai-routing   onboard   proxy-mode   retry-timeout-factor <50-200>   timeout]   preference] | <p>Configures a RADIUS accounting server</p> <ul style="list-style-type: none"> <li>&lt;1-6&gt; [dscp &lt;0-63&gt;   host &lt;WORD&gt;   nai-routing   onboard   proxy-mode   retry-timeout-factor &lt;50-200&gt;   timeout] – Selects a server value to configure <ul style="list-style-type: none"> <li>dscp &lt;0-63&gt; – Specifies a Differentiated Services Code point values (QoS) used in generated RADIUS packets <ul style="list-style-type: none"> <li>&lt;0-63&gt; – Enter a DSCP value between 0 and 63</li> </ul> </li> <li>host &lt;WORD&gt; – Displays the address of the server to be configured <ul style="list-style-type: none"> <li>&lt;WORD&gt; secret – Enter the IP address or hostname of the server <ul style="list-style-type: none"> <li>secret [0 &lt;WORD&gt;   2 &lt;WORD&gt;   &lt;WORD&gt;] {port} &lt;1-65535&gt; – Configures the RADIUS server shared secret <ul style="list-style-type: none"> <li>0 &lt;WORD&gt; – Enter a clear text secret</li> <li>2 &lt;WORD&gt; – Enter an encrypted text secret</li> <li>&lt;WORD&gt; {port} – Enter the shared secret, up to 127 characters</li> <li>{port} &lt;1-65535&gt; – Configures the authentication port</li> <li>&lt;1-65535&gt; – Configures the UDP port for accounting. The default port is 1812.</li> </ul> </li> </ul> </li> </ul> </li> <li>nai-routing realm-type – Configures Network Access Identifier based forwarding of requests <ul style="list-style-type: none"> <li>realm-type [prefix   suffix] – Select the match type made on the username <ul style="list-style-type: none"> <li>prefix realm &lt;WORD&gt; {strip} – Matches the prefix of the username (Eg: username is of type DOMAIN/user1, DOMAIN/user2)</li> <li>suffix realm &lt;WORD&gt; {strip} – Matches the suffix of the username</li> </ul> </li> </ul> </li> </ul> <p>The following parameters are common for both prefix and suffix:</p> <ul style="list-style-type: none"> <li>realm &lt;WORD&gt; – Enter the text matched against the username</li> <li>&lt;WORD&gt; {strip} – Enter the matching text including the delimiter (delimiter is typically " or '@') <ul style="list-style-type: none"> <li>{strip} – Strips the realm from the username before forwarding the request to the RADIUS server</li> </ul> </li> </ul> </li></ul> |

---

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• onboard [controller self] – Selects an onboard server instead of an external host           <ul style="list-style-type: none"> <li>• controller – Configures the controller’s RADIUS server to which the device is presently adopted</li> <li>• self – Indicates the device itself</li> </ul> </li> <li>• proxy-mode [none through-controller through-rf-domain-manager] – Select the mode of proxying requests from the list given below           <ul style="list-style-type: none"> <li>• none – No proxy required. Send the request directly using the IP address of the device</li> <li>• through-controller – Proxy the requests through the controller that is configuring the device</li> <li>• through-rf-domain-manager – Proxy the requests through the local rf-domain-manager</li> </ul> </li> <li>• retry-timeout-factor &lt;50-200&gt; – Configures the scaling of the retry timeout for this server between 50 and 200 seconds</li> <li>• timeout &lt;1-60&gt; {attempts} &lt;1-10&gt; – Configures the timeout in seconds for each request sent to the RADIUS server           <ul style="list-style-type: none"> <li>• attempts &lt;1-10&gt; – Displays the number of times a transmission request is attempted</li> </ul> </li> <li>• &lt;1-10&gt; – Enter the number of attempts between 1 and 10           <ul style="list-style-type: none"> <li>• preference [auth-server-host auth-server-number none] – Configures the process in which a server from the pool is selected for sending authentication requests.               <ul style="list-style-type: none"> <li>• auth-server-host – Prefers the same server host that was used for authentication</li> <li>• auth-server-number – Prefers the same index/number of the server that was used for authentication</li> <li>• none – Selects accounting server independent of which server was used for authentication</li> </ul> </li> </ul> </li> </ul> | <hr/> <p>Configures the type of RADIUS accounting packets sent</p> <ul style="list-style-type: none"> <li>• start-interim-stop – Sends Start message when the session begins, periodic Interim-Accounting updates, and finally an Accounting-Stop when the session ends</li> <li>• start-stop – Sends an Accounting-Start message when the session begins, and Accounting-Stop when the session ends</li> <li>• stop-only – Sends Accounting-Stop message when the session ends</li> </ul> <hr/> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Example**

```
RFController(config-aaa-policy-test)#accounting interim interval 65

RFController(config-aaa-policy-test)#accounting server 2 host 172.16.10.10
secret Brocade port 1

RFController(config-aaa-policy-test)#accounting server 2 nai-routing
realm-type prefix realm word strip

RFController(config-aaa-policy-test)#accounting server 2 host word secret word
port 6000

RFController(config-aaa-policy-test)#accounting server 2 timeout 2 attempts 2

RFController(config-aaa-policy-test)#accounting type start-stop

RFController(config-aaa-policy-test)#accounting server preference
auth-server-number
RFController(config-aaa-policy-test)#show context
aaa-policy test
  accounting server 1 host 172.16.10.100 secret 0 testing
  accounting server 2 host 172.16.10.10 secret 0 brocade port 1008
  accounting server 2 nai-routing realm-type prefix realm DSOS strip
  accounting type start-interim-stop
  accounting interim interval 65
  accounting server preference auth-server-number
```



## authentication

### *aaa-policy*

Configures authentication parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
authentication [eap|protocol|server]
authentication eap wireless-client [attempts <1-10>|identity-request-timeout
<1-60>|retry-timeout-factor <50-200>|timeout <1-60>]
authentication protocol [chap|pap]
authentication server <1-6> [dscp|host|nac|nai-routing|onboard|
proxy-mode|retry-timeout-factor <50-200>|timeout]
authentication server <1-6> host <WORD> secret [0 <WORD> | 2 <WORD>|<WORD>]
{port} <1-65535>
authentication server <1-6> nac
authentication server <1-6> nai-routing realm-type [prefix|suffix] realm
<WORD> {strip}
authentication server <1-6> onboard [controller|self]
authentication server <1-6> proxy-mode
[none|through-controller|through-rf-domain-manager]
authentication server <1-6> timeout <1-60300> {attempts} <1-100>
```

## Parameters

---

|                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>eap wireless-client [attempts &lt;1-10&gt;   identity-request-timeout &lt;1-60&gt;   retry-timeout-factor &lt;50-200&gt;   timeout &lt;1-60&gt; ]</pre> | <p>Configures EAP parameters for clients</p> <ul style="list-style-type: none"> <li>• wireless-client – Configures EAP wireless client related parameters <ul style="list-style-type: none"> <li>• attempts &lt;1-10&gt; – Enter the number of times a request is sent to a client <ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify the number of attempts</li> </ul> </li> <li>• identity-request-timeout &lt;1-60&gt; – Enter the timeout value after which an EAP-Identity request message to a client is retried <ul style="list-style-type: none"> <li>• &lt;1-60&gt; – Specify timeout in seconds</li> </ul> </li> <li>• retry-timeout-factor &lt;50-200&gt; – Configures the mode the successive EAP retries are arranged <ul style="list-style-type: none"> <li>• &lt;50-200&gt; – Enter the scaling factor between 50 and 200 seconds</li> </ul> </li> <li>• timeout &lt;1-60&gt; – Specifies the timeout after which a request to a client is retried <ul style="list-style-type: none"> <li>• &lt;1-60&gt; – Enter a timeout value between 1 and 60 seconds</li> </ul> </li> </ul> </li> </ul> |
| <pre>protocol [chap   pap]</pre>                                                                                                                             | <p>Configures the protocol used for non-EAP authentication</p> <ul style="list-style-type: none"> <li>• chap – Uses <i>Challenge Handshake Authentication Protocol</i> (CHAP)</li> <li>• pap – Uses <i>Password Authentication Protocol</i> (PAP)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

---

---

|                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>server &lt;1-6&gt; [ dscp host  nac nai-routing onboard proxy-m ode retry-timeout-factor &lt;50-200&gt; time-out]</pre> | <p>Configures an authentication server</p> <ul style="list-style-type: none"> <li>• &lt;1-6&gt; [ dscp host  nac nai-routing onboard proxy-mode retry-timeout-factor &lt;50-200&gt; time-out] – Selects a server to be configured <ul style="list-style-type: none"> <li>• dscp &lt;0-63&gt; – Specifies a differentiated devices code point value (QoS) to be used in generated RADIUS packets <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Configures a DSCP value between 0 and 3</li> </ul> </li> <li>• host &lt;WORD&gt; – Defines the address of the server <ul style="list-style-type: none"> <li>• &lt;WORD&gt; secret – Enter the IP address or hostname of the server <ul style="list-style-type: none"> <li>• secret [0 &lt;WORD&gt;   2 &lt;WORD&gt;   &lt;WORD&gt;] {port} &lt;1-65535&gt; – Configures the RADIUS server shared secret</li> <li>• 0 &lt;WORD&gt; – Enter a clear text secret</li> <li>• 2 &lt;WORD&gt; – Enter an encrypted text secret</li> <li>• &lt;WORD&gt; {port} – Enter the shared secret</li> <li>• {port} &lt;1-65535&gt; – Configures the authentication port</li> <li>• &lt;1-65535&gt; – Enter the UDP port used for authentication. The default port is 1812.</li> </ul> </li> </ul> </li> </ul> </li> <li>• nac – Uses the server for devices requiring network access control</li> <li>• nai-routing realm-type – Configures network access identifier based forwarding of requests <ul style="list-style-type: none"> <li>• realm-type [prefix suffix] – Select the match type made on the username <ul style="list-style-type: none"> <li>• prefix realm &lt;WORD&gt; {strip} – Matches the prefix of the username</li> <li>• suffix realm &lt;WORD&gt; {strip} – Matches the suffix of the username</li> </ul> </li> </ul> </li> </ul> <p>The following parameters are common for both prefix and suffix:</p> <ul style="list-style-type: none"> <li>• realm &lt;WORD&gt; – Enter the text to be matched against the username <ul style="list-style-type: none"> <li>• &lt;WORD&gt; {strip} – Enter the match text including the delimiter if applicable <ul style="list-style-type: none"> <li>• {strip} – Strips the realm from the username before forwarding the request to the RADIUS server</li> </ul> </li> </ul> </li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 
- onboard [controller|self] – Selects an onboard server instead of an external host
    - controller – Specifies the onboard server on the controller to which the AP is adopted
    - self – Specifies the onboard server on the device (AP or controller) where the client is associated
  - proxy-mode [none|through-controller|through-rf-domain-manager] – Selects the mode of proxying requests
    - none – Sends the requests directly using the IP address of the device without proxy
    - through-controller – Proxies the requests through the controller that is configuring the device
    - through-rf-domain-manager – Proxies the requests through the local rf-domain-manager
  - retry-timeout-factor <50-200> – Configures the scaling of the retry timeout for the server. Enter a timeout value between 50 and 200 seconds
  - timeout <1-60> – Enter the timeout for each request sent to the RADIUS server
    - <1-60> {attempts} – Enter the timeout in seconds
      - attempts <1-10> – Enter the number of times a request is sent to the RADIUS server
      - <1-10> – Enter the number of attempts required before a timeout
- 

### Example

```

RFController(config-aaa-policy-test)#authentication server 5 host 172.16.10.10
secret brocade port 1000
RFController(config-aaa-policy-test)#authentication server 5 timeout 10
attempts 3
RFController(config-aaa-policy-test)#authentication server 5 nai-routing realm
-type suffix realm @brocade.com strip
RFController(config-aaa-policy-test)#authentication protocol chap
RFController(config-aaa-policy-test)#authentication eap wireless-client
attempts 2
RFController(config-aaa-policy-test)#authentication eap wireless-client
identity-request-timeout 20
RFController(config-aaa-policy-test)#authentication server 2 onboard
controller
RFController(config-aaa-policy-test)#
RFController(config-aaa-policy-test)#show context
aaa-policy test
  authentication server 5 onboard controller
  authentication server 5 timeout 20
  authentication server 5 nai-routing realm-type suffix realm @brocade.com
strip
  accounting server 1 host 172.16.10.100 secret 0 testing
  accounting server 2 host 172.16.10.10 secret 0 brocade port 1008
  accounting server 2 nai-routing realm-type prefix realm DSOS strip
  authentication eap wireless-client identity-request-timeout 20
  authentication protocol chap
  accounting type start-interim-stop
  accounting interim interval 65
  accounting server preference auth-server-number
  authentication server 5 host 172.16.10.10 secret 0 brocade port 1009
  authentication server 5 timeout 20
  authentication server 5 host 172

```

## mac-address-format

### aaa-policy

Configures the format in which a MAC address must be filled in the RADIUS-request frames

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### 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 – Formatted as AABCC-DDEEFF              |
| [middle-hyphen no-delim      | • no-delim – Formatted as AABCCDDEEFF                    |
| pair-colon pair-hyphen       | • pair-colon – Formatted as AA:BB:CC:DD:EE:FF            |
| quad-dot] case [lower upper] | • pair-hyphen – Formatted as AA-BB-CC-DD-EE-FF (default) |
| attributes [all              | • quad-dot – Formatted as AAB.CCDD.EEF                   |
| username-password]           |                                                          |

The following parameters are common for all the above.

- case [lower|upper] – Specifies whether the MAC address is to be filled in upper or lower case
  - lower – Uses lower case (Eg: aa-bb-cc-dd-ee-ff)
  - upper – Uses upper case (Eg: AA-BB-CC-DD-EE-FF)
    - attributes[all|username-password] – Specifies which RADIUS attributes will use the customized MAC address format
    - all – All attributes with MAC addresses (Username, Password, Calling-Station-Id, Called-Station-Id)
    - username-password – Specifies the username and password fields (which have the MAC address when mac-auth is used)

---

### Example

```
RFController(config-aaa-policy-test)#mac-address-format quad-dot case upper at
tributes username-password
RFController(config-aaa-policy-test)#show context
aaa-policy test
mac-address-format quad-dot case upper attributes username-password
```

**no***aaa-policy*

Negates a command or sets its default values

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [accounting|authentication|mac-address-format|server-pooling-mode|use]
```

**Parameters**

|                     |                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------|
| accounting          | Configures accounting parameters                                                                      |
| authentication      | Configures authentication parameters                                                                  |
| mac-address-format  | Resets the MAC address format used in requests to the default format                                  |
| server-pooling-mode | Resets the method of selecting a server from the pool of configured AAA servers to its default values |
| use                 | Defines the settings used with this command                                                           |

**Usage Guidelines**

Removes an access list control entry. Provide the rule-precedence value when using the no command.

**Example**

```
RFController(config-aaa-policy-test)#no accounting dscp

RFController(config-aaa-policy-test)#no mac-address-format

RFController(config-aaa-policy-test)#no server-pooling-mode fail-through
RFController(config-aaa-policy-test)#no authentication server 3 proxy-mode
RFController(config-aaa-policy-test)#
```

## server-pooling-mode

### *aaa-policy*

Configures the method of selecting a server from the pool of configured AAA servers

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
server-pooling-mode [fail-over|load-balance]
```

### Parameters

|              |                                                               |
|--------------|---------------------------------------------------------------|
| fail-over    | Performs a failover starting from the first configured server |
| load-balance | Sends load-balance requests across all servers in the pool    |

### Example

```
RFController(config-aaa-policy-test)#server-pooling-mode load-balance
RFController(config-aaa-policy-test)#sho context
aaa-policy test
server-pooling-mode load-balance
```

## use

### *aaa-policy*

Applies a NAC for use by this aaa policy.

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
use nac-list <NAC-LIST>
```

### Parameters

---

|                     |                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------|
| nac-list <NAC-LIST> | Configures the Network Access Control related parameters                                                                     |
|                     | <ul style="list-style-type: none"> <li>• &lt;NAC-LIST&gt; – Enter an existing NAC list for use by this aaa-policy</li> </ul> |

---

### Example

```
RFController(config-aaa-policy-test)#use nac-list test1
RFController(config-aaa-policy-test)#show context
aaa-policy test
  server-pooling-mode load-balance
  use nac-list test1
```



## write

### *aaa-policy*

Writes the running configuration to memory or a terminal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
write [memory|terminal|memory]
```

### Parameters

|          |                      |
|----------|----------------------|
| memory   | Writes to NV memory  |
| terminal | Writes to a terminal |

### Example

```
RFController(config-aaa-policy-test)#write terminal
!
! Configuration of Mobility RFS7000 Controller version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
  assignable-power-range 8 9
!
wlan-qos-policy default
!
radio-qos-policy default
!
aaa-policy default
!
association-acl-policy default
!
wips-policy default
!
hotspot-policy default
!
firewall ratelimit-trust policy default
!
management-policy default
  telnet
  http server
  ssh
```

## 9 aaa-policy

```
!  
!  
firewall dos-attack policy default  
!  
firewall policy default  
!  
radius-server-policy default  
!  
mint-security-policy the_policy  
!  
role-policy default  
!  
device-discover-policy default  
!
```

## clrscr

### *aaa-policy*

Clears the screen's current display

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
clrscr
```

### **Parameters**

None

### **Example**

```
clrscr
```

## commit

### *aaa-policy*

Commits all the changes made in the active session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
commit {write}{memory}
```

### Parameters

|        |                                                                  |
|--------|------------------------------------------------------------------|
| write  | If a commit succeeds, the configuration is written to the memory |
| memory | Writes to memory                                                 |

### Example

```
RFController(config-aaa-policy-test)#commit write memory
[OK]
RFController(config-aaa-policy-test)#
```

## do

### *aaa-policy*

Runs the commands from EXEC mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
do <parameter>
```

### Parameters

---

|             |                                                                              |
|-------------|------------------------------------------------------------------------------|
| <parameter> | Displays parameters for which information can be viewed using the do command |
|-------------|------------------------------------------------------------------------------|

---

### Example

```
RFController(config-aaa-policy-test)#do ?

  ap-upgrade      AP firmware upgrade
  archive          Manage archive files
  boot             Boot commands
  cd               Change current directory
  change-passwd   Change password
  clear            Clear
  clock            Configure software system clock
  cluster          Cluster commands
  commit           Commit all changes made in this session
  configure        Enter configuration mode
  connect          Open a console connection to a remote device
  copy             Copy from one file to another
  crypto           Encryption related commands
  debug            Debugging functions
  delete           Deletes specified file from the system.
  diff             Display differences between two files
  dir              List files on a filesystem
  disable          Turn off privileged mode command
  edit             Edit a text file
  enable           Turn on privileged mode command
  erase            Erase a filesystem
  format           Format file system
  halt             Halt the system
  help             Description of the interactive help system
  logging          Modify message logging facilities
  mint            MiNT protocol
  mkdir            Create a directory
  more            Display the contents of a file
```

|               |                                                                                     |
|---------------|-------------------------------------------------------------------------------------|
| no            | Negate a command or set its defaults                                                |
| page          | Toggle paging                                                                       |
| ping          | Send ICMP echo messages                                                             |
| pwd           | Display current directory                                                           |
| reload        | Halt and perform a warm reboot                                                      |
| remote-debug  | Troubleshoot remote system(s)                                                       |
| rename        | Rename a file                                                                       |
| revert        | Revert changes                                                                      |
| rmdir         | Delete a directory                                                                  |
| self          | Config context of the device currently logged into                                  |
| telnet        | Open a telnet connection                                                            |
| terminal      | Set terminal line parameters                                                        |
| time-it       | Check how long a particular command took between request and completion of response |
| tracert       | Trace route to destination                                                          |
| upgrade       | Upgrade software image                                                              |
| upgrade-abort | Abort an ongoing upgrade                                                            |
| watch         | Repeat the specific CLI command at a periodic interval                              |
| write         | Write running configuration to memory or terminal                                   |
| clrscr        | Clears the display screen                                                           |
| exit          | Exit from the CLI                                                                   |
| service       | Service Commands                                                                    |
| show          | Show running system information                                                     |

## end

### *aaa-policy*

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
end
```

### **Parameters**

None

### **Example**

```
RFController(config-aaa-policy-test)#end  
RFController#
```

## exit

### *aaa-policy*

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
exit
```

### **Parameters**

None

### **Example**

```
RFController(config-aaa-policy-test)#exit  
RFController(config)#
```



## health-check

### *aaa-policy*

Configures server health-check parameters

Displays the interactive help system

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
health-check interval <60-86400>
```

### Parameters

---

interval <60-86400>

Configure an interval (in seconds) after which a server that was marked down earlier is checked again to see if it is now reachable

- <60-86400> – Interval in seconds
- 

### Example

```
RFController(config-aaa-policy-test)#health-check interval 4000
RFController(config-aaa-policy-test)#
```

## help

### *aaa-policy*

Displays the interactive help system

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
help search <WORD> {detailed|only-show|skip-show}
```

### Parameters

---

|               |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| search <WORD> | Looks for CLI commands related to a specific term<br><WORD> {detailed only-show skip-show} – A term to search CLI commands for (a feature or a configuration parameter)<br>detailed – Searches and displays help strings in addition to mode and commands<br>only-show – Displays only the "show" commands, not configuration commands<br>skip-show – Displays only configuration commands, not "show" commands |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-aaa-policy-test)#help
```

When using the CLI, help is provided at the command line when typing '?'.

If no help is available, the help content will be empty. Backup until entering a '?' shows the help content.

There are two styles of help provided:

1. Full help. Available when entering a command argument (e.g. 'show ?'). This will describe each possible argument.

2. Partial help. Available when an abbreviated argument is entered. This will display which arguments match the input (e.g. 'show ve ?').

```
RFController(config-aaa-policy-test)#
```

## revert

### *aaa-policy*

Reverts the changes made to their last saved configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
revert
```

### **Parameters**

None

### **Example**

```
RFController(config-aaa-policy-test)#revert  
RFController(config-aaa-policy-test)#
```

## service

### *aaa-policy*

Displays service commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
service show cli
```

### Parameters

|      |                                           |
|------|-------------------------------------------|
| show | Displays running system configuration     |
| cli  | Displays the CLI tree of the current mode |

### Example

```
RFController(config-aaa-policy-test)#service show cli
AAA Policy Mode mode:
+-help [help]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config)
(|include-factory)]
  +-session-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config)
(|include-factory)]
  +-device
    +-DEVICE [show device DEVICE (|include-factory)]
      +-include-factory [show device DEVICE (|include-factory)]
  +-session-changes [show session-changes]
  +-internal
    +-context
      +-running-config
        +-WORD [show internal context (running-config|session-config) WORD
(|include-factory)]
          +-include-factory [show internal context
(running-config|session-config) WORD (|include-factory)]
      +-session-config
        +-WORD [show internal context (running-config|session-config) WORD
(|include-factory)]
          +-include-factory [show internal context
(running-config|session-config) WORD (|include-factory)]
      +-startup-config [show startup-config (|include-factory)]
        +-include-factory [show startup-config (|include--DOMAIN-NAME [show
wireless mobile-unit (|(on DEVICE-OR-DOMAIN-NAME))]
```

```
+-mac
  +-AA-BB-CC-DD-EE-FF [show wireless mobile-unit mac AA-BB-CC-DD-EE-FF
(|(on DEVICE-OR-DOMAIN-NAME))]
+-on
  +-DEVICE-OR-DOMAIN-NAME [show wireless mobile-unit mac
AA-BB-CC-DD-EE-FF (|(on DEVICE-OR-DOMAIN-NAME))]
  +-statistics [show wireless mobile-unit statistics (|traffic) (|(on
DEVICE-OR-DOMAIN-NAME))].....
.....
RFController(config-aaa-policy-test)#
```

## show

### *aaa-policy*

Displays running system information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show <parameter>
```

### Parameters

None

### Example

|                       |                                                                |
|-----------------------|----------------------------------------------------------------|
| adoption              | Display information related to adoption to wireless controller |
| advanced-wips         | Advanced WIPS                                                  |
| ap-upgrade            | AP Upgrade                                                     |
| boot                  | Display boot configuration.                                    |
| captive-portal        | Captive portal commands                                        |
| cdp                   | Cisco Discovery Protocol                                       |
| clock                 | Display system clock                                           |
| cluster               | Cluster Protocol                                               |
| commands              | Show command lists                                             |
| context               | Information about current context                              |
| critical-resources    | Critical Resources                                             |
| crypto                | Encryption related commands                                    |
| debug                 | Debugging functions                                            |
| debugging             | Debugging functions                                            |
| device-categorization | Device Categorization                                          |
| event-history         | Display event history                                          |
| event-system-policy   | Display event system policy                                    |
| file                  | Display filesystem information                                 |
| firewall              | Wireless Firewall                                              |
| interface             | Interface Configuration/Statistics commands                    |
| ip                    | Internet Protocol (IP)                                         |
| ip-access-list-stats  | IP Access list stats                                           |
| licenses              | Show installed licenses and usage                              |
| lldp                  | Link Layer Discovery Protocol                                  |
| mac-access-list-stats | MAC Access list stats                                          |
| mac-address-table     | Display MAC address table                                      |
| mint                  | MiNT protocol                                                  |
| noc                   | Noc-level information                                          |
| ntp                   | Network time protocol                                          |
| password-encryption   | Password encryption                                            |
| power                 | Show power over ethernet command                               |

|                   |                                            |
|-------------------|--------------------------------------------|
| remote-debug      | Show details of remote debug sessions      |
| rf-domain-manager | Show RF Domain Manager selection details   |
| role              | Role based firewall                        |
| running-config    | Current operating configuration            |
| session-changes   | Configuration changes made in this session |
| session-config    | This session configuration                 |
| sessions          | Display CLI sessions                       |
| smart-rf          | Smart-RF Management Commands               |
| spanning-tree     | Display spanning tree information          |
| startup-config    | Startup configuration                      |
| terminal          | Display terminal configuration parameters  |
| timezone          | The timezone                               |
| upgrade-status    | Display last image upgrade status          |
| version           | Display software & hardware version        |
| wireless          | Wireless commands                          |

## 9 aaa-policy



# auto-provisioning-policy

---

## In this chapter

- [auto-provisioning-policy](#) ..... 576

This chapter summarizes the auto-provisioning-policy commands in the CLI structure.

Adoption rules are sorted by precedence value and matched (filtered) against the information available from an AP, any rule for the wrong AP type is ignored.

For example,

```
rule #1 adopt br7131 10 profile default vlan 10
rule #2 adopt br650 20 profile default vlan 20
rule #3 adopt br7131 30 profile default serial-number
xxx rule #4 adopt br7131 40 p d mac aa bb
```

Mobility 7131 Series Access Point L2 adoption, VLAN 10 - will use rule #1

Mobility 7131 Series Access Point L2 adoption, VLAN 20 - will not use rule #2 (wrong type), may use rule #3 if the serial number matched, else rule #4

If aa<= MAC <= bb, or else default.

Use the (config) instance to configure auto-provisioning-policy related configuration commands. To navigate to the auto-provisioning-policy instance, use the following commands:

```
RFController(config)#auto-provisioning-policy <policy-name>
RFController(config)#auto-provisioning-policy test1
RFController(config-auto-provisioning-policy-test1)#
Adoption Policy Mode commands:
adopt          Add rule for device adoption
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
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

RFController(config-auto-provisioning-policy-test)#
```

## auto-provisioning-policy

[Table 25](#) Summarizes auto-provisioning-policy commands

**TABLE 25** auto-provisioning-policy commands

| Command                          | Description                                                                                         | Reference                |
|----------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">adopt</a>            | Adds rules for device adoption                                                                      | <a href="#">page 577</a> |
| <a href="#">default-adoption</a> | Adopts devices even when no matching rules are found. Assigns default profile and default rf-domain | <a href="#">page 580</a> |
| <a href="#">deny</a>             | Adds a rule to deny device adoption                                                                 | <a href="#">page 581</a> |
| <a href="#">no</a>               | Negates a command or sets its default value                                                         | <a href="#">page 583</a> |

## adopt

### *auto-provisioning-policy*

Adds rules for device adoption

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
adopt [br71xx|br650|br6511|br6532]
```

```
adopt [br71xx|br650|br6511|br6532] <1-1000> <PROFILE>  
<RF-DOMAIN> [any|cdp-match <WORD>|dhcp-option <WORD>|fqdn <WORD>|ip|lldp-match  
<WORD>|mac|model-number <WORD>|serial-number <WORD>|vlan <VLAN-ID>]
```

```
adopt [br71xx|br650|br6511|br6532] <1-1000> <PROFILE>  
<RF-DOMAIN> ip [<Starting IP> <Ending IP>|<A.B.C.D/M>]
```

```
adopt [br71xx|br650|br6511|br6532] <1-1000> <PROFILE>  
<RF-DOMAIN> mac <Starting MAC> {<Ending MAC>}
```

## Parameters

```
adopt [br71xx|br650|br6511|
br6532] <1-1000> <PROFILE>
<RF-DOMAIN> [any|cdp-match
<WORD>|dhcp-option
<WORD>|fqdn
<WORD>|ip|lldp-match
<WORD>|mac|model-number
<WORD>|serial-number
<WORD>|vlan <VLAN-ID>]
```

Adds rules for device adoption

- br71xx – Configures a Mobility 7131 Series Access Point
- br650 – Configures a Mobility 650 Access Point
- br6511 – Configures a Mobility 6511 Access Point
- br6532 – Configures a Mobility 6532 Access Point

The following parameters are common for all the APs:

- <1-1000> – Configure a rule precedence value between 1 and 1000
- <PROFILE> – Enter the name of the profile to use
  - <RF-DOMAIN> – Enter the RF-Domain device to use
  - any – Matches any device
  - cdp-match <WORD> – Matches device location based on CDP snoop
  - <WORD> – Specify the location substring to match
  - dhcp-option <WORD> – Matches the value of DHCP option
  - <WORD> – Enter the DHCP option name
  - fqdn <WORD> – Matches the value of FQDN
  - <WORD> – Specify the value to match
  - ip [<Starting IP> <Ending IP>|<A.B.C.D/M>] – Matches device IP address
  - <Starting IP> <Ending IP> – Enter a beginning and an ending IP address range to configure
  - <A.B.C.D/M> – Enter the IP address to configure
  - lldp-match <WORD> – Matches device location based on LLDP snoop
  - <WORD> – Specify the location substring to match
  - mac <Starting MAC> <Ending MAC> – Matches device MAC address
  - <Starting MAC> <Ending MAC> – Enter a starting and ending MAC address from a range of MAC addresses. An ending MAC address is optional.
  - model number <WORD> – Matches device model number
  - <WORD> – Enter the matching device model number
  - serial-number <WORD> – Matches device serial number
  - <WORD> – Enter the matching device serial number
  - vlan <VLAN-ID> – Matches device VLAN
  - <VLAN-ID> – Enter a target VLAN ID

**Example**

```

RFController(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default vlan 1
RFController(config-auto-provisioning-policy-test)#commit write memory
RFController(config-auto-provisioning-policy-test)#show wireless ap
+-----+-----+-----+-----+-----+-----+-----+
|IDX| NAME           | MAC           |TYPE|SERIAL NUMBER|ADOPTION-MODE|VERSION|
+-----+-----+-----+-----+-----+-----+-----+
| 1 | br7131-889EC4 | 00-15-70-88-9E-C4 | BR7131 | 06 |L2: vlan1     |5.1.0.0|
+-----+-----+-----+-----+-----+-----+-----+

RFController(config-auto-provisioning-policy-test)#show wireless ap
configured
+-----+-----+-----+-----+-----+-----+
|  IDX |      NAME      |      MAC      |  PROFILE  |RF-DOMAIN |
+-----+-----+-----+-----+-----+-----+
|  1   | br7131-889EC4 | 00-15-70-88-9E-C4 | default-br7131 | default |
|  2   | br650-445566  | 11-22-33-44-55-66 | default-br650  | default |
+-----+-----+-----+-----+-----+-----+

RFController(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default dhcp-option test1

RFController(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default ip 172.16.10.3 172.16.10.4

RFController(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default ip 172.16.10.3/24

RFController(config-auto-provisioning-policy-test)#adopt br7131 10 br7131
default mac 11-22-33-44-55-66

RFController(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
adopt br7131 10 br7131 default vlan 1
RFController(config-auto-provisioning-policy-test)#

```

## default-adoption

### *auto-provisioning-policy*

Adopts devices even when no matching rules are found. Assigns a default profile and default RF-Domain

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
default-adoption
```

### **Parameters**

None

### **Example**

```
RFController(config-adoption-policy-test)#default-adoption
RFController(config-adoption-policy-test)#show context
auto-provisioning-policy test default-adoption
```

## deny

### *auto-provisioning-policy*

Adds a rule to deny device adoption

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
deny [br71xx|br650|br6511|br6532] <1-1000>  
[any|cdp-match <WORD>|dhcp-option <WORD>|fqdn <WORD>|ip|lldp-match  
<WORD>|mac|model-number <WORD>|serial-number <WORD>|vlan <VLAN-ID>]
```

```
deny [br71xx|br650|br6511|br6532] <1-1000> ip [<Starting IP> <Ending  
IP>|A.B.C.D/M]
```

```
deny [br71xx|br650|br6511|br6532] <1-1000> mac <Starting MAC> {<Ending MAC>}
```

## Parameters

---

|                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>[br7131 br650 br6511  br6532] &lt;1-1000&gt; [any cdp-match &lt;WORD&gt; dhcp-option &lt;WORD&gt; fqdn ip lldp-match &lt;WORD&gt; mac model-number &lt;WORD&gt; serial-number &lt;WORD&gt; vlan &lt;VLAN-ID&gt;]</pre> | <p>Use the 'deny' command to add a rule to deny a device adoption</p> <ul style="list-style-type: none"> <li>• br71xx – Configures a Mobility 7131 Series Access Point</li> <li>• br650 – Configures a Mobility 650 Access Point</li> <li>• br6511 – Configures a Mobility 6511 Access Point</li> <li>• br6532 – Configures a Mobility 6532 Access Point</li> </ul> <p>The following parameters are common for both Mobility 7131 Series Access Points and Mobility 650 Access Points:</p> <ul style="list-style-type: none"> <li>• &lt;1-1000&gt; – Configure a rule precedence value between 1 and 1000 <ul style="list-style-type: none"> <li>• any – Matches any device</li> <li>• cdp-match &lt;WORD&gt; – Matches device location based on CDP snoop <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the location substring to match</li> </ul> </li> <li>• dhcp option &lt;WORD&gt; – Matches the value of DHCP option <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter the DHCP option name</li> </ul> </li> <li>• fqdn &lt;WORD&gt; – Matches the value of FQDN <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the value to match</li> </ul> </li> <li>• ip [&lt;Starting IP&gt; &lt;Ending IP&gt; &lt;A.B.C.D/M&gt;] – Matches device IP address <ul style="list-style-type: none"> <li>• &lt;Starting IP&gt; &lt;Ending IP&gt; – Enter a beginning and an ending IP address range to configure</li> <li>• &lt;A.B.C.D/M&gt; – Enter the IP address to configure</li> </ul> </li> <li>• lldp-match &lt;WORD&gt; – Matches device location based on LLDP snoop <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the location substring to match</li> </ul> </li> <li>• mac &lt;Starting MAC &gt; {&lt;Ending MAC&gt;} – Matches device MAC address <ul style="list-style-type: none"> <li>• &lt;Starting MAC&gt; &lt;Ending MAC&gt; – Enter a starting and ending MAC address of a range on MAC addresses. Ending MAC address is optional.</li> </ul> </li> <li>• model number &lt;WORD&gt; – Matches device model number <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter the matching device model number</li> </ul> </li> <li>• serial number &lt;WORD&gt; – Matches device serial number <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter the matching device serial number</li> </ul> </li> <li>• vlan &lt;VLAN-ID&gt; – Matches device VLAN <ul style="list-style-type: none"> <li>• &lt;VLAN-ID&gt; – Enter a target VLAN ID</li> </ul> </li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Example

```
RFController(config-auto-provisioning-policy-test)#deny br71xx 600 vlan 1
RFController(config-auto-provisioning-policy-test)#deny br71xx 600 ip
172.16.10.1/24
RFController(config-auto-provisioning-policy-test)#show context
auto-provisioning-policy test
default-adoption
deny br71xx 100 vlan 20
deny br71xx 101 ip 172.16.11.0/24
```



## no

### *auto-provisioning-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [adopt | default-adoption | deny]
```

### Parameters

---

|                          |                                                                         |
|--------------------------|-------------------------------------------------------------------------|
| [adopt                   | • adopt – Removes an adoption rule                                      |
| default-adoption   deny] | • default-adoption – Does not adopt a device if no matching rules apply |
|                          | • deny – Removes a deny rule                                            |

---

### Example

```
RFController(config-auto-provisioning-policy-test1)#no default-adoption
RFController(config-auto-provisioning-policy-test1)#
```

### NOTE

The commands `clear`, `commit`, `exit`, `help`, `write`, `revert`, `service` and `show` are common commands. Refer to [Chapter 6, Common Commands](#) for more information.

---

## 10 auto-provisioning-policy

## advanced-wips-policy

### In this chapter

- [advanced-wips-policy](#) ..... 585

This chapter summarizes the advanced-wips-policy commands within the CLI structure.

Use the (config) instance to configure advanced-wips-policy related configuration commands. To navigate to the advanced-wips-policy instance, use the following commands:

```
RFController(config)#advanced-wips-policy <policy-name>
RFController(config)#advanced-wips-policy test
RFController(config-advanced-wips-policy-test)#
RFController(config-advanced-wips-policy-test)#?
Advanced WIPS policy Mode commands:
  event          Configure event detection
  no             Negate a command or set its defaults
  server-listen-port  Configure local WIPS server listen port number
  terminate      Add a device to the list of devices to be terminated
  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
RFController(config-advanced-wips-policy-test)#
```

## advanced-wips-policy

[Table 26](#) Summarizes advanced-wips-policy commands

**TABLE 26** advanced-wips-policy Commands

| Command                            | Description                                 | Reference                |
|------------------------------------|---------------------------------------------|--------------------------|
| <a href="#">event</a>              | Configures events                           | <a href="#">page 587</a> |
| <a href="#">no</a>                 | Negates a command or sets its default value | <a href="#">page 592</a> |
| <a href="#">server-listen-port</a> | Sets a local WIPS server's listening port   | <a href="#">page 593</a> |

**TABLE 26** advanced-wips-policy Commands

| Command                   | Description                                             | Reference                |
|---------------------------|---------------------------------------------------------|--------------------------|
| <a href="#">terminate</a> | Adds a device to a list of devices terminated           | <a href="#">page 594</a> |
| <a href="#">use</a>       | Defines the settings used with the advanced-wips-policy | <a href="#">page 595</a> |

## event

### *advanced-wips-policy*

Configures event detection. Configures the parameters related to the detection of anomalous frames on the RF network.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
event [accidental-association|all|
crackable-wep-iv-used|dos-cts-flood|
dos-deauthentication-detection|dos-disassociation-detection|dos-eap-failure-s
poof|dos-eapol-logoff-storm|dos-rts-flood|
essid-jack-attack-detected| fake-dhcp-server-detected|fata-jack-detected|
id-theft-eapol-success-spoof-detected|
id-theft-out-of-sequence|invalid-channel-advertized|invalid-management-frame|
ipx-detection|monkey-jack-attack-detected|
multicast-all-routers-on-subnet|multicast-all-systems-on-subnet|
multicast-dhcp-server-relay-agent|multicast-hsrp-agent|multicast-igmp-detecti
on|multicast-igmp-routers-detection|
multicast-ospf-all-routers-detection|multicast-ospf-designated-routers-detect
ion|multicast-rip2-routers-detection|
multicast-vrrp-agent|netbios-detection|
null-probe-response-detected|probe-response-flood | rogue-ap-detection|
stp-detection|unauthorized-bridge|windows-zero-config-memory-leak|wlan-jack-a
ttack-detected]
```

```
event [accidental-association|rogue-ap-detection|unauthorized-bridge]
[mitigation-enable|trigger-against {neighboring/sanctioned/unsanctioned}]
```

```
event all trigger-all-applicable
event crackable-wep-iv-used trigger-against
{neighboring/sanctioned/unsanctioned}
event dos-cts-flood [threshold [cts-frames-ratio |
mu-rx-cts-frames]<0-65535> |trigger-against
{neighboring/sanctioned/unsanctioned}]
```

```
event [dos-deauthentication-detection|dos-disassociation-detection|
dos-eap-failure-spoof|dos-rts-flood|essid-jack-attack-detected|fake-dhcp-serv
er-detected|fata-jack-detected|id-theft-eapol-success-spoof-detected|id-theft
-out-of-sequence|invalid-channel-advertized|invalid-management-frame|ipx-dete
ction|monkey-jack-attack-detected|multicast-all-routers-on-subnet|multicast-a
ll-systems-on-subnet|multicast-dhcp-server-relay-agent|multicast-hsrp-agent|m
ulticast-igmp-detection|multicast-igmp-routers-detection|multicast-ospf-all-r
```

## 11 advanced-wips-policy

```
outers-detection|multicast-ospf-designated-routers-detection|multicast-rip2-routers-detection|multicast-vrrp-agent|netbios-detection|null-probe-response-detected|stp-detection|windows-zero-config-memory-leak|wlan-jack-attack-detected] trigger-against{neighboring/sanctioned/unsanctioned}
```

```
event dos-eapol-logoff-storm [threshold  
[eapol-start-frames-ap|eapol-start-frames-mu]<0-65535> |trigger-against  
{neighboring/sanctioned/unsanctioned}]  
event probe-response-flood [threshold probe-rsp-frames-count  
<0-65535>|trigger-against {neighboring/sanctioned/unsanctioned}]
```

## Parameters

|                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>event<br/>[accidental-association   rogue-ap-detection   unauthorized-bridge]<br/>[mitigation-enable   trigger-against {neighboring   sanctioned   unsanctioned}]</p> | <p>Configures parameters related to the detection of anomalous frames on the RF network. The parameters are:</p> <ul style="list-style-type: none"> <li>• accidental-association – Detects an accidental client association</li> <li>• rogue-ap-detection – Detects a rogue AP</li> <li>• unauthorized-bridge – Detects an unauthorized bridge</li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• mitigation-enable – Enables the mitigation for the event</li> <li>• trigger-against {neighboring   sanctioned   unsanctioned} – Sets a trigger from the list <ul style="list-style-type: none"> <li>• neighboring – Triggers against neighboring (ignored) devices</li> <li>• sanctioned – Triggers against sanctioned (approved) devices</li> <li>• unsanctioned – Triggers against unsanctioned (unapproved) devices</li> </ul> </li> </ul> |
| <p>all trigger-all-applicable</p>                                                                                                                                        | <p>Detects all the events</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p>dos-cts-flood [threshold [cts-frames-ratio   mu-rx-cts-frames] &lt;0-65535&gt;   trigger-against {neighboring   sanctioned   unsanctioned}]</p>                       | <p>Detects DoS CTS Flood</p> <ul style="list-style-type: none"> <li>• threshold [cts-frames-ratio   mu-rx-cts-frames] – Configures the event's threshold <ul style="list-style-type: none"> <li>• cts-frames-ratio &lt;0-65535&gt; – CTS/Total Frames ratio in percentage</li> <li>• mu-rx-cts-frames &lt;0-65535&gt; – Threshold for CTS frames received by a client <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Specify a threshold value between 0 and 65535</li> </ul> </li> </ul> </li> <li>• trigger-against {neighboring   sanctioned   unsanctioned} – Sets the trigger from the list <ul style="list-style-type: none"> <li>• neighboring – Triggers against neighboring (ignored) devices</li> <li>• sanctioned – Triggers against sanctioned (approved) devices</li> <li>• unsanctioned – Triggers against unsanctioned (unapproved) devices</li> </ul> </li> </ul>              |

---

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[crackable-wep-iv-used   dos-deauthentication-detection   dos-disassociation-detection   dos-eap-failure-spoof   dos-rtts-flood   essid-jack-attack-detected   fake-dhcp-server-detected   fata-jack-detected   id-theft-eapol-success-spoof-detected   id-theft-out-of-sequence   invalid-management-frame   ipx-detection   monkey-jack-attack-detected   multicast-all-routers-on-subnet   multicast-all-systems-on-subnet   multicast-dhcp-server-relay-agent   multicast-hsrp-agent   multicast-igmp-detection   multicast-igmp-routers-detection   multicast-ospf-all-routers-detection   multicast-ospf-designated-routers-detection   multicast-rip2-routers-detection</p> | <ul style="list-style-type: none"> <li>• crackable-wep-iv-used – Detects crackable WEP IV used</li> <li>• dos-deauthentication-detection – Detects DoS deauthentication</li> <li>• dos-disassociation-detection – Detects DoS disassociation</li> <li>• dos-eap-failure-spoof – Detects a DoS EAP failure spoof</li> <li>• dos-rtts-flood – Detects a DoS RTSflood</li> <li>• essid-jack-attack-detected – Detects an ESSID jack attack</li> <li>• fake-dhcp-server-detected – Detects a fake DHCP server</li> <li>• fata-jack-detected – Detects a fata-jack attack</li> <li>• id-theft-eapol-success-spoof-detected – Detects an ID theft - EAPOL success spoof</li> <li>• id-theft-out-of-sequence – Detects an ID theft - out of sequence</li> <li>• invalid-channel-advertized – Detects an invalid channel advertizement</li> <li>• invalid-management-frame – Detects an invalid management frame</li> <li>• ipx-detection – Detects IPX</li> <li>• monkey-jack-attack-detected – Detects a monkey-jack attack</li> <li>• multicast-all-routers-on-subnet – Detects all multicast routers in the subnet</li> <li>• multicast-all-systems-on-subnet – Detects all multicast systems on the subnet</li> <li>• multicast-dhcp-server-relay-agent – Detects multicast DHCP server relay agents</li> <li>• multicast-hsrp-agent – Detects multicast HSRP agents</li> <li>• multicast-igmp-detection – Detects multicast IGMP</li> <li>• multicast-igmp-routers-detection – Detects multicast IGRP routers</li> <li>• multicast-ospf-all-routers-detection – Detects multicast OSPF all routers</li> </ul> |
| <p>multicast-vrrp-agent   netbios-detection   null-probe-response-detected   stp-detection   windows-zero-config-multicast-rip2-routers-detection   memory-leak   wlan-jack-attack-detected ] trigger-against {neighboring   sanctioned   unsanctioned}</p>                                                                                                                                                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• multicast-ospf-designated-routers-detection – Detects multicast OSPF designated routers</li> <li>• multicast-rip2-routers-detection – Detects multicast RIP2 routers</li> <li>• multicast-vrrp-agent – Detects multicast VRRP agents</li> <li>• netbios-detection – Detects NetBIOS</li> <li>• null-probe-response-detected – Detects null probe response</li> <li>• stp-detection – Detects STP</li> <li>• windows-zero-config-memory-leak – Detects windows zero config memory leak</li> <li>• wlan-jack-attack-detected – Detects WLAN jack attacks</li> </ul> <p>The following parameters are common for all the above:</p> <ul style="list-style-type: none"> <li>• trigger-against{neighboring   sanctioned   unsanctioned – Sets the trigger from the list             <ul style="list-style-type: none"> <li>• neighboring – Triggers against Neighboring (Ignored) devices</li> <li>• sanctioned – Triggers against Sanctioned (sanctioned) devices</li> <li>• unsanctioned – Triggers against Unsanctioned (Unsanctioned) devices</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |



---

|                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>dos-eapol-logoff-storm [threshold [eapol-start-frames-ap eapol-start-frames-mu]&lt;0-65535&gt;  trigger-against {neighboring sanctioned unsanctioned}]</pre> | <p>Detects DoS EAPoL Logoff Storm</p> <ul style="list-style-type: none"> <li>• threshold – Configures the event threshold <ul style="list-style-type: none"> <li>• eapol-start-frames-ap &lt;0-65535&gt; – Detects EAPoL start frames transmitted by an AP</li> <li>• eapol-start-frames-mu &lt;0-65535&gt; – Detects EAPoL start frames transmitted by a client <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Select a threshold value between 0 and 65535</li> </ul> </li> </ul> </li> <li>• trigger-against{neighboring sanctioned unsanctioned} – Sets the trigger from the list <ul style="list-style-type: none"> <li>• neighboring – Triggers against neighboring ignored) devices</li> <li>• sanctioned – Triggers against sanctioned (approved) devices</li> <li>• unsanctioned – Triggers against unsanctioned (unapproved) devices</li> </ul> </li> </ul> |
| <pre>probe-response-flood [threshold probe-rsp-frames-count &lt;0-65535&gt; trigger-against {neighboring  sanctioned unsanctioned}]</pre>                         | <p>Detects Probe Response Flood values</p> <ul style="list-style-type: none"> <li>• threshold probe-rsp-frames-count &lt;0-65535&gt; – Configures the event threshold <ul style="list-style-type: none"> <li>• probe-rsp-frames-count &lt;0-65535&gt; – Count for probe response frames transmitted by an AP <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Select a threshold value between 0 and 65535</li> </ul> </li> </ul> </li> <li>• trigger-against{neighboring sanctioned unsanctioned} – Sets the trigger from the list <ul style="list-style-type: none"> <li>• neighboring – Trigger against neighboring (ignored) devices</li> <li>• sanctioned – Trigger against sanctioned (approved) devices</li> <li>• unsanctioned – Trigger against unsanctioned (unapproved) devices</li> </ul> </li> </ul>                                                       |

---

### Example

```
RFController(config-advanced-wips-policy-test)#event dos-cts-flood threshold
cts-frames-ratio 8
```

```
RFController(config-advanced-wips-policy-test)#event dos-eapol-logoff-storm
threshold eapol-start-frames-mu 99
```

```
RFController(config-advanced-wips-policy-test)#event probe-response-flood
threshold probe-rsp-frames-count 8
```

```
RFController(config-advanced-wips-policy-test)#event
wlan-jack-attack-detected trigger-against sanctioned
```

```
RFController(config-advanced-wips-policy-test)#event probe-response-flood
trigger-against sanctioned
```

## no

### *advanced-wips-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [event|server-listen-port|terminate|use]
```

### Parameters

|                    |                                                       |
|--------------------|-------------------------------------------------------|
| event              | Configures event detection                            |
| server-listen-port | Sets a local WIPS server's listen port                |
| terminate          | Removes a device from the device termination list     |
| use                | Defines settings to use with the advanced WIPS policy |

### Example

```
RFController(config-advanced-wips-policy-test)#no event  
accidental-association trigger-against
```

```
RFController(config-advanced-wips-policy-test)#no server-listen-port
```

## server-listen-port

### *advanced-wips-policy*

Configures the local WIPS server's listening port

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
server-listen-port <0-65535>
```

### Parameters

---

|                              |                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------|
| server-listen-port <0-65535> | Select a port number between 0 and 65535 for the WIPS sensors to connect to the server |
|------------------------------|----------------------------------------------------------------------------------------|

---

### NOTE

Onboard WIPS uses port 8443 and AirDefense Enterprise uses 443

---

### Example

```
RFController(config-advanced-wips-policy-test)#server-listen-port 1009
```

## terminate

### *advanced-wips-policy*

Adds a device to the termination list

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
terminate <AA-BB-CC-DD-EE-FF>
```

### Parameters

---

```
terminate <AA-BB-CC-DD-EE-FF>
```

Specify a target termination device MAC address in the AA-BB-CC-DD-EE-FF format

---

### Example

```
RFController(config-advanced-wips-policy-test)#terminate 00-40-96-B0-BA-2D
```

## USE

### *advanced-wips-policy*

Sets the device categorizations settings for the specified device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
use device-categorization <WORD>
```

### Parameters

---

|                              |                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| device-categorization <WORD> | Creates/Configures device categorization list                                                                             |
|                              | <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a device name to be associated to this profile</li> </ul> |

---

### NOTE

advanced-wips ignores SSID of marked devices for device-categorization

### Example

```
RFController(config-advanced-wips-policy-test)#use device-categorization
rfs7000
Please note, advanced-wips ignores the SSID of marked devices
RFController(config-advanced-wips-policy-test)#
```

### NOTE

The commands `clrscr`, `commit`, `exit`, `help`, `write`, `revert`, `service` and `show` are common commands. For more information, see [Chapter 6, Common Commands](#).

## 11 advanced-wips-policy

# association-acl-policy

## In this chapter

- [association-acl-policy](#) ..... 597

This chapter summarizes the association-acl-policy commands within the CLI structure.

Use the (config) instance to configure association-acl-policy related configuration commands. To navigate to the association-acl-policy instance, use the following commands:

```
RFController(config)#association-acl-policy <policy-name>
RFController(config-assoc-acl-test)# association-acl-policy test
RFController(config-assoc-acl-test)#
RFController(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
RFController(config-assoc-acl-test)#
```

## association-acl-policy

[Table 27](#) Summarizes association-acl-policy commands

**TABLE 27** association-acl-policy commands

| Command                | Description                                  | Reference                |
|------------------------|----------------------------------------------|--------------------------|
| <a href="#">deny</a>   | Specifies a range of denied MAC addresses    | <a href="#">page 598</a> |
| <a href="#">no</a>     | Negates a command or sets its default value  | <a href="#">page 599</a> |
| <a href="#">permit</a> | Specifies a range of permitted MAC addresses | <a href="#">page 600</a> |

## deny

### *association-acl-policy*

Specifies a range of denied MAC addresses

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
deny <Starting-MAC> [<Ending-MAC>|precedence <1-1000>]
deny <Starting-MAC> <Ending-MAC> precedence <1-1000>
```

### Parameters

---

|                                    |                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Starting-MAC>                     | Enter the starting MAC address in a range of denied MAC addresses                                                                                                                                                                                                                                                                            |
| [<Ending-MAC> precedence <1-1000>] | <ul style="list-style-type: none"> <li>• &lt;Ending-MAC&gt; precedence &lt;1-1000&gt; – Enter the ending MAC address of a range of MAC addresses. (Optional if a single MAC is added)</li> <li>• precedence &lt;1-1000&gt; – Enter a precedence value between 1 and 1000 (rules are checked in an increasing order of precedence)</li> </ul> |

---

### Example

```
RFController(config-assoc-acl-test)#deny 00-40-96-B0-BA-2D precedence 2
RFController(config-assoc-acl-test)#
```



## no

### *association-acl-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [deny|permit]
```

### Parameters

---

|               |                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| [deny permit] | <ul style="list-style-type: none"><li>• deny – Enter a deny rule to delete</li><li>• permit – Enter a permit rule to delete</li></ul> |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-assoc-acl-test)#no deny 00-40-96-B0-BA-2D precedence 2
RFController(config-assoc-acl-test)#
```

## permit

### *association-acl-policy*

Specifies a range of permitted MAC addresses

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

permit <Starting-MAC> [<Ending-MAC>|precedence <1-1000>]
permit <Starting-MAC> <Ending-MAC> precedence <1-1000>

```

### Parameters

---

|                                    |                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Starting-MAC>                     | Enter the starting MAC address in a range of permitted MAC addresses                                                                                                                                                                                                                                                                       |
| [<Ending-MAC> precedence <1-1000>] | <ul style="list-style-type: none"> <li>• &lt;Ending-MAC&gt; precedence &lt;1-1000&gt; – Enter the ending MAC address in a range of MAC addresses. Optional if a single MAC is added</li> <li>• precedence &lt;1-1000&gt; – Enter a precedence value between 1 and 1000 (rules are checked in an increasing order of precedence)</li> </ul> |

---

### Example

```

RFController(config-assoc-acl-test)#permit 00-40-96-B0-BA-2D precedence 3
RFController(config-assoc-acl-test)#

```

### NOTE

clrscr, commit, do, exit, help, write, revert, service and show are common commands. For more information, see [Chapter 6, Common Commands](#).

---

## access-list

## In this chapter

- [ip-access-list](#) ..... 602
- [mac-access-list](#) ..... 625

This chapter summarizes IP and MAC Access list commands in detail.

Access-lists control access to the network through a set of rules. Each rule specifies an action taken when a packet matches a given set of rules. If the action is deny, the packet is dropped. If the action is permit, the packet is allowed. The controller supports the following ACLs.

- IP access lists
- MAC access lists

Use an 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 access-list related configuration commands. To navigate to the (config-access-list) instance, use the following commands.

*ip-access-list*

```
RFController(config)#ip access-list test
RFController(config-ip-acl-acl)#?
ACL Config 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
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
RFController(config-ip-acl-acl)#
```

*mac-access-list*

```

RFController(config)#mac access-list test
RFController(config-mac-acl-test)#?
MAC Extended ACL Config 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
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
RFController(config-mac-acl-test)#

```

## ip-access-list

Table 28 Summarizes commands under the IP access list mode

**TABLE 28** ip-access-list commands

| Command        | Description                                                                           | Reference               |
|----------------|---------------------------------------------------------------------------------------|-------------------------|
| <i>deny</i>    | Specifies packets to reject                                                           | <a href="#">page603</a> |
| <i>permit</i>  | Permits specific packets                                                              | <a href="#">page608</a> |
| <i>no</i>      | Negates a command or sets its default value                                           | <a href="#">page613</a> |
| <i>write</i>   | Writes information to memory or terminal                                              | <a href="#">page614</a> |
| <i>clrscr</i>  | Clears the display screen                                                             | <a href="#">page616</a> |
| <i>commit</i>  | Commits the changes made in the current session                                       | <a href="#">page617</a> |
| <i>end</i>     | Ends and exits the current mode and moves to the PRIV EXEC mode                       | <a href="#">page618</a> |
| <i>exit</i>    | Ends the current mode and moves to the previous mode                                  | <a href="#">page619</a> |
| <i>help</i>    | Displays the interactive help system                                                  | <a href="#">page620</a> |
| <i>revert</i>  | Reverts changes made to their last saved configuration                                | <a href="#">page621</a> |
| <i>service</i> | Invokes service commands to troubleshoot or debug (config-if) instance configurations | <a href="#">page622</a> |
| <i>show</i>    | Displays running system information                                                   | <a href="#">page624</a> |

## deny

*ip-access-list*

Specifies packets to reject

---

### NOTE

Use a decimal value representation of ethertypes to implement a permit/deny designation for a packet. The command set for IP ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
deny [icmp|ip|proto|tcp|udp]
```

```
deny icmp [<source-IP>|any|host <IP>] [<dest-IP>|any|host <IP>] {<ICMP-type>
{<ICMP-code>}} {log} {rule-precedence <1-5000>}] <0-255>
```

```
deny ip [<source-IP>|any|host <IP>] [<dest-IP>|any|host <IP>] {log}
{rule-precedence <1-5000>}
```

```
deny [tcp|udp] [<source-IP>|any|host <IP>] {eq
<source-port>|range <starting-source-port>
<ending-source-port>} [<dest-IP>|any|host <IP>]
{eq <source-port>} {range <starting-source-port>
<ending-source-port>} {eq[<1-65535>|<WORD>|bgp/dns/ftp/ftp
/gopher/https/ldap/nntp/ntp/pop3/smtp/ssh | telnet |tftp| www]} {log}
{rule-precedence <1-5000>}
```

```
deny proto
[<0-254>|<WORD>|eigrp|gre|igmp|igmp|ospf|vrrp][<source-IP/Mask>|any|host
<IP>][<dest-IP/Mask>|any|host <IP>] {log} {rule-description
<WORD>|rule-precedence<1-5000>}
```

## Parameters

|                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>deny ip [&lt;source-IP&gt;   any   host &lt;IP&gt;][&lt;dest-IP&gt;   any   host &lt;IP&gt;] {log} {rule-precedence &lt;1-5000&gt;}</pre>                                            | <p>Use with the deny command to reject packets</p> <ul style="list-style-type: none"> <li>• deny – Sets the action type on a ACL</li> <li>• IP – Specifies an IP address</li> <li>• &lt;source-ip&gt;   any   host &lt;IP&gt; – The keyword &lt;source-IP&gt; is the source IP address of the network or host in dotted decimal format.</li> <li>• any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0</li> <li>• host – host is an abbreviation for the exact source &lt;ip&gt; (A.B.C.D format) and source-mask bits equal to 32</li> <li>• &lt;dest-IP&gt;   any   host &lt;IP&gt; – Defines the destination host IP address or destination network address</li> <li>• log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs</li> <li>• rule-precedence &lt;1-5000&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL</li> </ul>                                                                                                                                                                                                                          |
| <pre>deny icmp [&lt;source-IP&gt;   any   host &lt;IP&gt;] [&lt;dest-IP&gt;   any   host &lt;IP&gt;] {&lt;ICMP-type&gt; {&lt;ICMP-code&gt;}} {log} {rule-precedence &lt;1-5000&gt;}</pre> | <p>Use with the deny command to reject ICMP packets</p> <ul style="list-style-type: none"> <li>• deny – Rejects ICMP packets</li> <li>• icmp – Specifies ICMP as the protocol</li> <li>• &lt;source-ip&gt;   any   host &lt;IP&gt;] – The source &lt;source-IP&gt; is the source IP address of the network or host (in dotted decimal format)</li> <li>• any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0</li> <li>• host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32</li> <li>• &lt;dest-IP&gt;   any   host &lt;IP&gt;] – Defines the destination host IP address or destination network address</li> <li>• &lt;ICMP-type&gt; {&lt;ICMP-code&gt;} – Sets the ICMP type value &lt;ICMP-type&gt; from 0 to 255, and is valid only for ICMP. The ICMP code value &lt;ICMP-code&gt; is from 0 to 255, and is valid only for ICMP</li> <li>• log – Generates log messages when a packet coming from an interface matches an ACL entry. Log messages are generated only for router ACLs only</li> <li>• rule-precedence &lt;1-5000&gt; – Optional. Defines an integer value between 1-5000. This value sets the rule precedence in the ACL</li> </ul> |

```
deny [tcp|udp]
 [<source-IP>|any|host <IP>] {eq
 <source-port>|range
 <starting-source-port>
 <ending-source-port>}
 [<dest-IP>|any|host <IP>]{eq
 <source-port>} {range
 <starting-source-port>
 <ending-source-port>} {eq
 <1-65535> |
 <WORD>|bgp|dns|ftp|ftp
 |gopher|https|ldap|nntp|ntp|po
 p3|smtp|ssh | telnet |tftp|
 www}{log} {rule-precedence
 <1-5000>}
```

Use with the deny command to reject TCP or UDP packets

- deny – Rejects TCP or UDP packets
- [tcp|udp] – Specifies TCP or UDP as the protocol
- <source-IP>|any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format)
- any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0
- host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32
- eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535
- range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers)
- <dest-IP>|any|host <IP> – Defines the destination host IP address or destination network address
- eq <source-port> {range <starting-source-port> <ending-source-port>} – Defines a specific destination port
- range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535
- <1-65535> – Destination port
- <WORD> – Displays any Service Name
- bgp – Bgp port 179
- dns – DNS port 53
- ftp – Ftp-ctrl port 21
- ftp-data – Ftp-data port 20
- gopher – Gopher port 70
- https – HTTPS port 443
- ldap – LDAP port 389
- nntp – NNTP port 119
- ntp – NTP port 123
- pop3 – Pop3 port 110
- smtp – SMTP port 25
- ssh – SSH port 22
- telnet – Telnet port 23
- tftp – TFTP port 69
- www – HTTP port 80
- log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs
- rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL

```
[<0-254> | <WORD> |
eigrp | gre | igmp | igp | ospf | vrrp] [
<source-IP/Mask> | any | host
<IP>] [<dest-IP/Mask> | any | host
<IP>] {log} {rule-description
<WORD> | rule-precedence <1-500
0>}]
```

Use with the deny command to deny any protocol other than TCP, UDP or ICMP

- <0-254> – Displays the protocol number
- <WORD> – Refers to any protocol name
- eigrp – EIGRP protocol 88
- gre – GRE protocol 47
- igmp – IGMP protocol 2
- igp – IGP protocol 9
- ospf – OSPF protocol 89
- vrrp – VRRP protocol 112
- <source-IP/Mask> | any | host <IP> – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching
- any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0
- host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32
- <dest-IP/mask> | any | host <IP> – Defines the destination host IP address or destination network address
- log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs
  - rule-precedence <1-5000> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL
  - rule-description <WORD> – Defines access-list entry name

### 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

The last 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/denied based on the ACL configuration.

- Filtering TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP as the protocol to allow/deny ICMP packets. Selecting ICMP provides the option of filtering ICMP packets based on ICMP type and code

### NOTE

The log option is functional only for router ACLs. The log option displays an informational logging message about the packet that matches the entry sent to the console.



**Example**

```
RFController(config-ip-acl-test)#deny icmp 172.16.10.3/24 any rule-precedence
88
RFController(config-ip-acl-test)#
RFController(config-ip-acl-test)#deny icmp 172.16.10.3/24 host 172.16.10.7 8
log rule-precedence 99
RFController(config-ip-acl-test)#
```

## permit

### *ip-access-list*

Permits specific packets

---

#### NOTE

Use a decimal value representation of ethertypes to implement a permit/deny designation for a packet. The command set for IP ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
permit[icmp|ip|tcp|udp|proto]
permit proto
[<0-255>|<WORD>|eigrp|gre|igmp|igp|ospf|vrrp][<source-IP/Mask>|any
|host <IP>][<dest-IP/Mask>|any|host <IP>] {log} {rule-description
<WORD>/rule-precedence<1-5000>} {mark [8021p <0-7>|
dscp <0-63>]}{rule-description <WORD>/rule-precedence<1-5000>}}
```

```
permit [tcp|udp] [<source-IP/Mask>|host <IP>|any] [<dest-IP/Mask>|host
<IP>|any] {eq <1-65535> | range <1-65535> <1-65535>} {eq [<1-65535> |
<WORD>|bgp/dns/ftp/ftp |gopher/https/ldap/nntp/ntp/pop3/smtp/ssh | telnet
/tftp/ www]}|range <1-65535>|log|mark [8021p <0-7>|dscp <0-63>] rule-precedence
<1-5000> {rule-description} <WORD> |rule-precedence <1-5000>
{rule-description} <WORD>}
```

```
permit [icmp|ip] [<source-IP/Mask>|any|host <IP>] [<dest-IP/Mask>|any|host
<IP>] {any[<0-255> <0-255>]} {log} {mark [8021p <0-7>|dscp<0-63>
rule-precedence <1-5000> {rule-description} <WORD> } {rule-precedence <1-5000>
{rule-description} <WORD>}
```

## Parameters

|                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>permit ip [&lt;source-IP/Mask&gt;   any   host &lt;IP&gt;] [&lt;dest-IP/Mask&gt;   any   host &lt;IP&gt;] {log} {rule-precedence &lt;1-5000&gt;} {mark [8021p &lt;0-7&gt;   dscp&lt;0-63&gt; rule-precedence &lt;1-5000&gt; {rule-description} &lt;WORD&gt; }</pre>                                            | <p>Use with a permit command to allow IP packets</p> <ul style="list-style-type: none"> <li>• permit – Sets the action type on an ACL</li> <li>• IP – Specifies an IP (to match to a protocol)</li> <li>• &lt;source-IP/Mask&gt;   any   host &lt;IP&gt; – The keyword &lt;source-IP&gt; is the source IP address of the network or host in dotted decimal format</li> <li>• any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0</li> <li>• host – host is an abbreviation for the exact source &lt;IP&gt; (A.B.C.D format) and source-mask bits equal to 32</li> <li>• &lt;dest-IP/Mask&gt;   any   host &lt;IP&gt; – Defines the destination host IP address or destination network address</li> <li>• log – Generates log messages when the packet coming from an interface matches an ACL entry. Log messages are generated only for router ACLs</li> <li>• rule-precedence &lt;1-5000&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL</li> <li>• mark – Use with mark command to mark a packet</li> <li>• 8012p &lt;0-7&gt; – Sets the 802.1p VLAN user priority value to &lt;vlan-priority-value&gt; (0-7)</li> <li>• dscp &lt;0-63&gt; – Sets the Differentiated Services Code Point code-point value to &lt;dscp-codepoint-value&gt; (0-63)</li> </ul>                                                                                                                                                                                                                                                  |
| <pre>permit icmp [&lt;source-IP/Mask&gt;   any   host &lt;ip&gt;] [&lt;dest-IP/Mask&gt;   any   host &lt;IP&gt;] {&lt;ICMP-type&gt; {&lt;ICMP-code&gt;}} {log} {rule-precedence &lt;1-5000&gt;}} {mark [8021p &lt;0-7&gt;   dscp&lt;0-63&gt; rule-precedence &lt;1-5000&gt; {rule-description} &lt;WORD&gt; }</pre> | <p>Use with the permit command to allow ICMP packets</p> <ul style="list-style-type: none"> <li>• deny – Permits ICMP packets</li> <li>• icmp – Specifies ICMP as the protocol</li> <li>• [&lt;source-IP&gt;   any   host &lt;IP&gt;] – The &lt;source-IP&gt; is the source IP address of the network or host (in dotted decimal format).</li> <li>• any – any is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0</li> <li>• host – host is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32</li> </ul> <hr/> <ul style="list-style-type: none"> <li>• [&lt;dest-IP&gt;   any   host &lt;IP&gt;] – Defines the destination host IP address or destination network address</li> <li>• &lt;ICMP-type&gt; {&lt;ICMP-code&gt;} – Sets the ICMP type value &lt;ICMP-type&gt; from 0 to 255, and is valid only for ICMP. The ICMP code value &lt;ICMP-code&gt; is from 0 to 255, and is valid only for protocol type icmp</li> <li>• log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs</li> <li>• rule-precedence &lt;1-5000&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL</li> <li>• mark – Use with mark command to mark a packet</li> <li>• 8012p &lt;0-7&gt; – Sets the 802.1p VLAN user priority value to &lt;vlan-priority-value&gt; (0-7)</li> <li>• dscp &lt;0-63&gt; – Sets the Differentiated Services Code Point (DSCP) code-point value to &lt;dscp-codepoint-value&gt; (0-63)</li> </ul> |

```

permit [tcp|udp]
 [<source-ip/Mask> |any|host
 <IP>] {eq <source-port>|range
 <starting-source-port>
 <ending-source-port>}
 [<dest-IP/Mask> |any|host <IP>]
 {eq <source-port>} {range
 <starting-source-port>
 <ending-source-port>} {log}
 {rule-precedence
 <1-5000>}{mark [8021p
 <0-7>|dscp<0-63>
 rule-precedence <1-5000>
 {rule-description} <WORD> }

```

Use with the permit command to allow TCP or UDP packets

- permit – Permits TCP/UDP packets
- [tcp|udp] – Specifies TCP or UDP as the protocol
- <source-IP/Mask> |any|host <IP> – The source is the source IP address of the network or host (in dotted decimal format)
- any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0
- host – host is an abbreviation for the exact source (A.B.C.D) and the source-mask bits equal to 32
- eq <source-port> – The source port <source-port> to match. Values in the range 1 to 65535
- range <starting-source-port> <ending-source-port> – Specifies the protocol range (starting and ending protocol numbers)
- <dest-IP/Mask> |any|host <IP> – Defines the destination host IP address or destination network address
- eq <source-port> {range <starting-source-port> <ending-source-port> | word | bgp | dns | ftp | ftp-data | gopher | https | ldap | nntp | ntp | pop3 | smtp | ssh | telnet | tftp | www} – Defines a specific destination port to match
  - range <starting-source-port> <ending-source-port> – Specifies the destination port or range of ports. Port values are in the range of 1 to 65535
  - <1-65535> – Destination port
  - <WORD> – Displays any service name
  - bgp – Bgp port 179
  - dns – DNS port 53
  - ftp – Ftp-ctrl port 21
  - ftp-data – Ftp-data port 20
  - gopher – Gopher port 70
  - https – HTTPS port 443
  - ldap – LDAP port 389
  - nntp – NNTP port 119
  - ntp – NTP port 123
  - pop3 – Pop3 port 110
  - smtp – SMTP port 25
  - ssh – SSH port 22
  - telnet – Telnet port 23
  - tftp – TFTP port 69
  - www – HTTP port 80
- mark – Use with mark command to mark a packet
- 8012p <0-7> – Sets the 802.1p VLAN user priority value to <vlan-priority-value> (0-7)
- dscp <0-63> – Sets the Differentiated Services Code Point (DSCP) code-point value to <dscp-codepoint-value> (0-63)

---

|                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> permit proto  [&lt;0-254&gt;  WORD eigrp gre   igmp igp ospf vrrp]  [&lt;source-IP/Mask&gt;  any  host  &lt;IP&gt;][&lt;dest-IP/Mask&gt;  any  host  &lt;IP&gt;] {log} {rule-description  &lt;WORD&gt;  rule-precedence  &lt;1-5000&gt;} </pre> | <p>Use with the permit command to allow any protocol other than TCP, UDP or ICMP</p> <ul style="list-style-type: none"> <li>• 0-254] – Displays protocol number</li> <li>• &lt;WORD&gt; – Refers to any protocol name</li> <li>• eigrp – EIGRP protocol 88</li> <li>• gre – GRE protocol 47</li> <li>• igmp – IGMP protocol 2</li> <li>• igp – IGP protocol 9</li> <li>• ospf – OSPF protocol 89</li> <li>• vrrp – VRRP protocol 112</li> <li>• &lt;source-IP/Mask&gt;  any  host &lt;IP&gt; – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching</li> <li>• &lt;source-IP/Mask&gt;  any  host &lt;IP&gt; – The source is the source IP address of the network or host (in dotted decimal format). The source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.</li> <li>• any – any is an abbreviation for a source IP of 0.0.0.0, and the source-mask bits are equal to 0</li> <li>• host – host is an abbreviation for exact source (A.B.C.D) and the source-mask bits equal to 32</li> <li>• &lt;dest-IP/mask&gt;  any  host &lt;IP&gt; – Defines the destination host IP address or destination network address</li> <li>• log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs</li> <li>• rule-precedence &lt;1-5000&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL</li> <li>• rule-description &lt;WORD&gt; – Defines access-list entry name</li> </ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### 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

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 based on the ACL configuration.

- Filtering on TCP/UDP allows the user to specify port numbers as filtering criteria
- Select ICMP to allow/deny packets.
- Selecting ICMP allows to filter ICMP packets based on type and node.

---

### NOTE

The log option is functional only for router ACLs. The log option displays an informational logging message about the packet matching the entry sent to the console.

---

## Example

```
RFController(config-ip-acl-test)#permit icmp any any log rule-precedence 200
RFController(config-ip-acl-test)#

RFController(config-ip-acl-test)#permit ip 192.168.1.10/24 192.168.2.0/24
rule-precedence 40
RFController(config-ip-acl-test)#

RFController(config-ip-acl-test)# permit proto eigrp any any mark 8021p 2
rule-precedence 2
RFController(config-ip-acl-test)#
```

## no

### *ip-access-list*

Negates a command or sets its default

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [deny|permit]
```

### Parameters

|        |                              |
|--------|------------------------------|
| deny   | Specifies packets to reject  |
| permit | Specifies packets to forward |

### Usage Guidelines

Removes an access list control entry. Provide the rule-precedence value when using the no command.

### Example

```
RFController(config-ip-acl-test)#no mark 8021p 5 tcp 192.168.2.0/24 any
rule-precedence 10

RFController(config-ip-acl-test)#no permit ip any any rule-precedence 10

RFController(config-ip-acl-test)#no deny icmp any any rule-precedence 10
```

## write

### *ip-access-list*

Writes running configuration to memory or terminal

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
write [terminal|memory]
```

### Parameters

|          |                      |
|----------|----------------------|
| terminal | Writes to a terminal |
| memory   | Writes to memory     |

### Example

```
RFController(config-ip-acl-test)#write terminal
!
! Configuration of Mobility RFS7000 Controller version 5.1.0.0
!
! version 2.0
!
!
smart-rf-policy default
!
smart-rf-policy test
  assignable-power-range 8 9
!
wlan-qos-policy default
!
radio-qos-policy default
!
aaa-policy default
!
association-acl-policy default
!
wips-policy default
!
hotspot-policy default
!
firewall ratelimit-trust policy default
!
management-policy default
  telnet
  http server
  ssh
```



```
!  
!  
firewall dos-attack policy default  
!  
firewall policy default  
!  
radius-server-policy default  
!  
mint-security-policy the_policy  
!  
role-policy default  
!  
device-discover-policy default  
!
```

## clrscr

*ip-access-list*

Clears the display screen

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
clrscr
```

### Parameters

None

### Example

```
RFController(config-ip-acl-test)#clrscr  
RFController(config-ip-acl-test)#
```

## commit

### *ip-access-list*

Commits all changes made in the current session

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
commit {write} {memory}
```

### Parameters

|        |                                                              |
|--------|--------------------------------------------------------------|
| write  | If a commit succeeds, the configuration is written to memory |
| memory | Writes to memory                                             |

### Example

```
RFController(config-ip-acl-test)#commit write memory
[OK]
RFController(config-ip-acl-test)#
```

## end

### *ip-access-list*

Ends and exits the current mode and moves to the PRIV EXEC mode

The prompt changes to `RFController#`

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
end
```

### **Parameters**

None

### **Example**

```
RFController(config-ip-acl-test)#end  
RFController#
```

## exit

### *ip-access-list*

Ends the current mode and moves to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFController(config)#`

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
exit
```

### Parameters

None

### Example

```
RFController(config-ip-acl-test)#exit  
RFController(config-ip-acl-test)#
```

## help

### *ip-access-list*

Displays the interactive help system

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
help
```

### **Parameters**

None

### **Example**

```
RFController(config-ip-acl-test)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.
```

If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input e.g. 'show ve?'.)

```
RFController(config-ip-acl-test)#
```

## revert

### *ip-access-list*

Reverts any updates to their last saved configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
revert
```

### Parameters

None

### Example

```
RFController(config-ip-acl-test)#revert  
RFController(config-ip-acl-test)#
```

## service

### *ip-access-list*

Displays service commands

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
service show cli
```

### Parameters

|      |                                           |
|------|-------------------------------------------|
| show | Displays running system configuration     |
| cli  | Displays the CLI tree of the current mode |

### Example

```
RFController(config-ip-acl-test)#service show cli
AAA Policy Mode mode:
+-help [help]
+-show
  +-commands [show commands]
  +-running-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config)
(|include-factory)]
  +-session-config [show (running-config|session-config) (|include-factory)]
    +-include-factory [show (running-config|session-config)
(|include-factory)]
  +-device
    +-DEVICE [show device DEVICE (|include-factory)]
      +-include-factory [show device DEVICE (|include-factory)]
  +-session-changes [show session-changes]
  +-internal
    +-context
      +-running-config
        +-WORD [show internal context (running-config|session-config) WORD
(|include-factory)]
          +-include-factory [show internal context
(running-config|session-config) WORD (|include-factory)]
      +-session-config
        +-WORD [show internal context (running-config|session-config) WORD
(|include-factory)]
          +-include-factory [show internal context
(running-config|session-config) WORD (|include-factory)]
      +-startup-config [show startup-config (|include-factory)]
        +-include-factory [show startup-config (|include--DOMAIN-NAME [show
wireless mobile-unit (|(on DEVICE-OR-DOMAIN-NAME))]]
```



```

+-mac
  +-AA-BB-CC-DD-EE-FF [show wireless mobile-unit mac AA-BB-CC-DD-EE-FF
(|(on DEVICE-OR-DOMAIN-NAME))]
+-on
  +-DEVICE-OR-DOMAIN-NAME [show wireless mobile-unit mac
AA-BB-CC-DD-EE-FF (|(on DEVICE-OR-DOMAIN-NAME))]
  +-statistics [show wireless mobile-unit statistics (|traffic) (|(on
DEVICE-OR-DOMAIN-NAME))].....
.....
RFController(config-ip-acl-test)#

```

## show

### *ip-access-list*

Displays running system information

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
show <parameter>
```

### Parameters

None

### Example

```
RFController(config-ip-acl-test)#show ?
aclstats          ACL stats
adoption          Display information related to adoption
advanced-wips     Advanced WIPS
boot             Display boot configuration.
clock            Display system clock
commands         Show command lists
context          Information about current context
crypto           Encryption related commands
debugging        Debugging functions
device           Device configuration
event-history     Display event history
file             Display filesystem information
firewall         Wireless Firewall
hotspot          Hotspot functions
interface        Interface Configuration/Statistics commands
ip              Internet Protocol (IP)
mint             MiNT protocol
ntp             Network time protocol
role            Role based firewall
running-config   Current operating configuration
session-changes  Configuration changes made in this session
session-config   This session configuration
smart-rf         Smart-RF Management Commands
startup-config   Startup configuration
terminal        Display terminal configuration parameters
upgrade-status   Display last image upgrade status
version          Display software & hardware version
wireless        Wireless commands
RFController(config-ip-acl-test)#
```

## mac-access-list

[Table 29](#) Summarizes MAC Access list commands

**TABLE 29** mac-access-list commands

| Command                | Description                                   | Reference               |
|------------------------|-----------------------------------------------|-------------------------|
| <a href="#">permit</a> | Use this command to specify packets to accept | <a href="#">page626</a> |
| <a href="#">deny</a>   | Use this command to specify packets to reject | <a href="#">page632</a> |

## permit

*mac-access-list*

Specifies packets to forward

---

### NOTE

Use a decimal value representation of ethertypes to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
permit [ <source-MAC> | any | host ]
```

```
permit <source-MAC> <AA-BB-CC-DD-EE-FF> <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p
<0-7>|log|mark [8021p<0-7>|dscp<0-63>[rule-precedence
<1-5000>[rule-description <WORD>]]|rule-precedence <1-5000>[rule-description
<WORD>|type [8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]
[log|rule-precedence <1-5000> rule-description <WORD>]|vlan <1-4095>
[log|rule-precedence|type[8021q|
<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]
```

```
permit [any|host] <dest-MAC> <dest-mask> [dot1p <0-7>|log|mark
[8021p<0-7>|dscp<0-63>[rule-precedence <1-5000>[rule-description
<WORD>]]|rule-precedence <1-5000>[rule-description <WORD>|type
[8021q|<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]
[log|rule-precedence]|vlan <1-4095> [log|rule-precedence<1-5000>
rule-description <WORD>|type[8021q|
<1-65535>|aarp|appletalk|arp|ip|ipv6|ipx|mint|rarp|wisp]]
```

## Parameters

| permit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Use with a permit command to allow IP packets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> permit &lt;source-MAC&gt; &lt;AA-BB-CC-DD-EE-FF&gt; &lt;dest-MAC&gt; &lt;AA-BB-CC-DD-EE-FF&gt; [dot1p &lt;0-7&gt;] [log] mark [8021p&lt;0-7&gt;] [dscp&lt;0-63&gt;] [rule-precedence &lt;1-5000&gt;] [rule-description &lt;WORD&gt;]]] rule-precedence &lt;1-5000&gt; [rule-description &lt;WORD&gt;]   type [8021q   &lt;1-65535&gt;]   aarp   appletalk   arp   ip   ipv6   ipx   mint   rarp   wisp] [log] rule-precedence &lt;1-5000&gt; rule-description &lt;WORD&gt;]]   vlan &lt;1-4095&gt; [log] rule-precedence   type [8021q   &lt;1-65535&gt;]   aarp   appletalk   arp   ip   ipv6   ipx   mint   rarp   wisp] </pre> | <ul style="list-style-type: none"> <li>• permit – Sets the ACL action type</li> <li>• &lt;source-MAC&gt; – Specify a source MAC address to match</li> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; – Specify a source MAC address mask</li> <li>• &lt;dest-MAC&gt; – Defines the destination MAC address</li> <li>• any – any destination host <ul style="list-style-type: none"> <li>• host – Defines the exact destination MAC address to match <ul style="list-style-type: none"> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; – Defines the source MAC address mask</li> <li>• dot1p &lt;0-7&gt; [log] rule-precedence   type] – 802.1p priority <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Priority value</li> </ul> </li> <li>• log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs</li> <li>• mark <ul style="list-style-type: none"> <li>• [8021p&lt;0-7&gt;] [dscp&lt;0-63&gt;] [rule-precedence &lt;1-5000&gt;] [rule-description &lt;WORD&gt;]] – Specifies packets to mark <ul style="list-style-type: none"> <li>• 8021p &lt;0-7&gt; – Modifies 802.1p VLAN user priority. Select a VLAN user VLAN user priority value</li> <li>• dscp &lt;0-63&gt; – Sets the Differentiated Services Code Point (DSCP) code-point value to &lt;dscp-codepoint-value&gt; (0-63)</li> <li>• &lt;0-63&gt; – Specify a DSCP codepoint value from 0-63</li> </ul> </li> <li>• rule-precedence&lt;1-5000&gt;rule-description &lt;WORD&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL <ul style="list-style-type: none"> <li>• rule-description – Access-list entry description</li> <li>• &lt;WORD&gt; – Specify the description up to 128 characters</li> </ul> </li> </ul> </li> <li>• type[8021q   &lt;1-65535&gt;]   aarp   appletalk   arp   ip   ip v6   ipx   mint   rarp   wisp] [log &lt;0-7&gt;]   rule-precedence &lt;1-5000&gt;] – Ether Type <ul style="list-style-type: none"> <li>• 8021q – VLAN Ether Type (0x8100)</li> <li>• &lt;1-65535&gt; – Ethernet protocol number</li> </ul> </li> </ul> </li> </ul> </li></ul> |

- 
- aarp – AARP Ether Type (0x80F3)
  - appletalk – APPLETALK Ether Type (0x809B)
  - arp – ARP Ether Type (0x0806)
  - ip – IP Ether Type (0x0800)
  - ipv6 – IPv6 Ether Type (0x86DD)
  - ipx – IPX Ether Type (0x8137)
  - mint – MINT Ether Type (0x8783)
  - rarp – RARP Ether Type (0x8035)
  - wisp – WISP Ether Type (0x8783)
  - vlan <1-4095> [log] rule-precedence <1-5000> rule-description <WORD> [type] – VLAN ID
    - <1-4095> – Specify a VLAN ID ID between 1-4095

```

any <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p
<0-7> | log] mark
[8021p<0-7> | dscp<0-63>][rule-precedence
<1-5000>][rule-description
<WORD>]]rule-precedence
<1-5000>[rule-description <WORD> | type
[8021q | <1-65535> | aarp | appletalk |
arp | ip | ipv6 | ipx | mint | rarp | wisp]
[log | rule-precedence] | vlan <1-4095>
[log | rule-precedence | type[8021q |
<1-65535> | aarp | appletalk |
arp | ip | ipv6 | ipx | mint | rarp | wisp]

```

any – Specify any source host to match

- <dest-MAC> – Defines the destination MAC address
- <AA-BB-CC-DD-EE-FF> – Defines the destination MAC address mask to match
  - host – Defines exact destination MAC address to match
    - AA-BB-CC-DD-EE-FF – Defines the source MAC address mask
    - dot1p <0-7> [log | rule-precedence | type] – 802.1p priority
      - <0-7> – priority value
    - log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs
    - mark
      - [8021p<0-7> | dscp<0-63>][rule-precedence <1-5000>][rule-description <WORD>]] – Use with mark command to mark a packet
        - 8021p <0-7> – Modifies 802.1p VLAN user priority. Select a VLAN user priority value
        - dscp <0-63> – Sets the differentiated services code-point value to <dscp-codepoint-value> (0-63)
        - <0-63> – Specify a DSCP codepoint value from 0-63
    - rule-precedence <1-5000> rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL
      - rule-description – Access-list entry description
      - <WORD> – Specify the description not exceeding 128 characters
  - type[8021q | <1-65535> | aarp | appletalk | arp | ip | ip v6 | ipx | mint | rarp | wisp][log<0-7> | rule-precedence <1-5000>] – Ether Type
    - 8021q – VLAN Ether Type (0x8100)
    - <1-65535> – Ethernet Protocol number
    - aarp – AARP Ether Type (0x80F3)
    - appletalk – APPLETALK Ether Type (0x809B)
    - arp – ARP Ether Type (0x0806)
    - ip – IP Ether Type (0x0800)
    - ipv6 – IPv6 Ether Type (0x86DD)
    - ipx – IPX Ether Type (0x8137)
    - mint – MINT Ether Type (0x8783)
    - rarp – RARP Ether Type (0x8035)
    - wisp – WISP Ether Type (0x8783)
- vlan <1-4095> [log | rule-precedence <1-5000> rule-description <WORD> | type – VLAN ID
  - <1-4095> – Specify a VLAN ID value between 1-4095

|                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>host &lt;source-MAC&gt; &lt;dest-MAC&gt; &lt;AA-BB-CC-DD-EE-FF&gt; [dot1p &lt;0-7&gt;   log   mark [8021p&lt;0-7&gt;   dscp&lt;0-63&gt;][rule-precedence &lt;1-5000&gt;][rule-description &lt;WORD&gt;]]   rule-precedence &lt;1-5000&gt;][rule-description &lt;WORD&gt;   type [8021q   &lt;1-65535&gt;   aarp   appletalk   arp   ip   ipv6   ipx   mint   rarp   wisp]] [log   mark   rule-precedence]</pre> | <p>Defines exact source address to match</p> <ul style="list-style-type: none"> <li>• &lt;source-MAC&gt; – Defines source MAC address to match</li> <li>• &lt;dest-MAC&gt; – Defines destination MAC address to match</li> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; – Defines destination MAC address mask to match <ul style="list-style-type: none"> <li>• dot1p &lt;0-7&gt; [log   rule-precedence   type] – 802.1p priority <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – priority value</li> </ul> </li> <li>• log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs</li> <li>• mark [8021p&lt;0-7&gt;   dscp&lt;0-63&gt;][rule-precedence &lt;1-5000&gt;][rule-description &lt;WORD&gt;] – Specifies packets to mark <ul style="list-style-type: none"> <li>• dscp &lt;0-63&gt; – Sets the Differentiated Services Code Point (DSCP) code-point value to &lt;dscp-codepoint-value&gt; (0-63) <ul style="list-style-type: none"> <li>• &lt;0-63&gt; – Specify a DSCP codepoint value from 0-63</li> </ul> </li> <li>• 8021p &lt;0-7&gt; – Modifies 802.1p VLAN user priority. Select a VLAN user VLAN user priority value</li> <li>• rule-precedence&lt;1-5000&gt;rule-description &lt;WORD&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL <ul style="list-style-type: none"> <li>• rule-description – Access-list entry description</li> </ul> </li> </ul> </li> </ul> </li></ul> |
|                                                                                                                                                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the description not exceeding 128 characters</li> </ul> <hr/> <ul style="list-style-type: none"> <li>• rule-precedence &lt;1-5000&gt; rule-description &lt;WORD&gt; – Defines an integer value between 1-5000 to set the rule precedence in the ACL <ul style="list-style-type: none"> <li>• rule-description – Access-list entry description</li> <li>• &lt;WORD&gt; – Specify the description not exceeding 128 characters</li> </ul> </li> <li>• type[8021q   &lt;1-65535&gt;   aarp   appletalk   arp   ip   ipv6   ipx   mint   rarp   wisp] [log &lt;0-7&gt;   rule-precedence &lt;1-5000&gt;][log   mark   rule-precedence] – Ether Type <ul style="list-style-type: none"> <li>• 8021q – VLAN Ether Type (0x8100)</li> <li>• &lt;1-65535&gt; – Ethernet protocol number</li> <li>• aarp – AARP Ether Type (0x80F3)</li> <li>• appletalk – APPLETALK Ether Type (0x809B)</li> <li>• arp – ARP Ether Type (0x0806)</li> <li>• ip – IP Ether Type (0x0800)</li> <li>• ipv6 – IPv6 Ether Type (0x86DD)</li> <li>• ipx – IPX Ether Type (0x8137)</li> <li>• mint – MiNT Ether Type (0x8783)</li> <li>• rarp – RARP Ether Type (0x8035)</li> <li>• wisp – WISP Ether Type (0x8783)</li> </ul> </li> <li>• vlan &lt;1-4095&gt; [log   rule-precedence &lt;1-5000&gt; rule-description &lt;WORD&gt;   type] – VLAN ID <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; – Specify a VLAN ID value between 1-4095</li> </ul> </li> </ul>                 |



The following parameters are common for all the 'Ethertype' parameters:

|                                                                                 |                                                                                                                                        |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| log                                                                             | Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs |
| mark [8021p<0-7>   dscp <0-63>[rule-precedence <1-5000>[rule-description <WORD> | Specifies packets to mark                                                                                                              |
| rule-precedence <1-5000><br>rule-description <WORD>                             | Defines an integer value between 1-5000. This value sets the rule precedence in the ACL                                                |

### Usage Guidelines

The permit command in the MAC ACL disallows 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

The controller (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access point through an interface, configure an access control list 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 ACLs.

### 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

```
RFController(config-mac-acl-test)#permit any any vlan 2 log rule-precedence 5
rule-description testrule
RFController(config-mac-acl-test)#
```

## deny

*mac-access-list*

Specifies packets to reject

---

**NOTE**

Use a decimal value representation of ethertypes to implement a `permit/deny` designation for a packet. The command set for MAC ACLs provide the hexadecimal values for each listed ethertype. The controller supports all ethertypes. Use the decimal equivalent of the ethertype listed for any other ethertype.

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
deny [<source-MAC> | any | host ]
```

```
deny <source-MAC> <AA-BB-CC-DD-EE-FF> <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p
<0-7> | log | rule-precedence <1-5000> [rule-description <WORD> | type
[8021q | <1-65535> | aarp | appletalk | arp | ip | ipv6 | ipx | mint | rarp | wisp]
[log | rule-precedence <1-5000> rule-desription <WORD>] | vlan <1-4095>
[log | rule-precedence | type [8021q | <1-65535> | aarp | appletalk | arp | ip |
ipv6 | ipx | mint | rarp | wisp]]
```

```
deny [any | host] <dest-MAC> <dest-mask> [dot1p <0-7> | log | rule-precedence
<1-5000> [rule-description <WORD> | type [8021q | <1-65535> | aarp | appletalk |
arp | ip | ipv6 | ipx | mint | rarp | wisp] [log | rule-precedence] | vlan <1-4095>
[log | rule-precedence <1-5000> rule-description
<WORD> | type [8021q | <1-65535> | aarp | appletalk |
arp | ip | ipv6 | ipx | mint | rarp | wisp]]
```

**Parameters**

| deny                        | Use with the deny command to reject packets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| deny [<source-MAC> any host | <ul style="list-style-type: none"> <li>• deny – Sets the action type on a ACL</li> <li>• &lt;source-MAC&gt; – Specify the source MAC address</li> <li>• &lt;AA-BB-CC-DD-EE-FF&gt; – Specify the source MAC address mask</li> <li>• &lt;dest-MAC&gt; – Specify the destination MAC address</li> <li>• any – any destination host <ul style="list-style-type: none"> <li>• host – host is an abbreviation for the exact source &lt;MAC Address&gt; (AA-BB-CC-DD-EE-FF format) and source-mask bits equal to 32 <ul style="list-style-type: none"> <li>• AA-BB-CC-DD-EE-FF – Specify the source MAC address mask</li> </ul> </li> <li>• dot1p &lt;0-7&gt; [log rule-precedence type] – Sets the 802.1p priority value <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Set the priority value from 0-7</li> </ul> </li> <li>• log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs.</li> <li>• rule-precedence&lt;1-5000&gt;rule-description &lt;WORD&gt; – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; – Specify a precedence value from 1-5000</li> <li>• rule-description – Access-list entry description</li> <li>• &lt;WORD&gt; – Enter the description not exceeding 128 characters</li> </ul> </li> <li>• type[8021q &lt;1-65535&gt; aarp appletalk arp ip ipv6 ipx mint rarp wisp] [log &lt;0-7&gt; rule-precedence &lt;1-5000&gt;] – Specifies various Ether types <ul style="list-style-type: none"> <li>• 8021q – VLAN Ether Type (0x8100)</li> <li>• &lt;1-65535&gt; – Ethernet Protocol number</li> <li>• aarp – AARP Ether Type (0x80F3)</li> <li>• appletalk – APPLETALK Ether Type (0x809B)</li> <li>• arp – ARP Ether Type (0x0806)</li> <li>• ip – IP Ether Type (0x0800)</li> <li>• ipv6 – IPv6 Ether Type (0x86DD)</li> <li>• ipx – IPX Ether Type (0x8137)</li> <li>• mint – MINT Ether Type (0x8783)</li> <li>• rarp – RARP Ether Type (0x8035)</li> <li>• wisp – WISP Ether Type (0x8783)</li> </ul> </li> <li>• vlan &lt;1-4095&gt; [log rule-precedence &lt;1-5000&gt;rule-description &lt;WORD&gt; type] – VLAN ID <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; – Specify a VLAN ID from 1-4095</li> </ul> </li> </ul> </li> </ul> |

- 
- any <dest-MAC> <AA-BB-CC-DD-EE-FF> [dot1p <0-7>] [log] rule-precedence <1-5000> [rule-description <WORD>] type [8021q | <1-65535> | aarp | appletalk | arp | ip | ipv6 | ipx | mint | rarp | wisp] [log] rule-precedence] vlan <1-4095> [log] rule-precedence | type [8021q | <1-65535> | aarp | appletalk | arp | ip | ipv6 | ipx | mint | rarp | wisp]
- any <dest-MAC> – Specify a destination MAC address
- <AA-BB-CC-DD-EE-FF> – Specify any destination MAC address mask
    - dot1p <0-7> – Sets the 802.1p priority value from 0-7
      - log – Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs.
      - rule-precedence <1-5000> rule-description <WORD> – Defines an integer value between 1-5000. This value sets the rule precedence in the ACL
        - rule-description – Access-list entry description
        - <WORD> – Enter the description not exceeding 128 characters
    - type [8021q | <1-65535> | aarp | appletalk | arp | ip | ipv6 | ipx | mint | rarp | wisp] [log <0-7>] rule-precedence <1-5000>] – Specify the EtherType
      - 8021q – VLAN Ether Type (0x8100)
      - <1-65535> – Ethernet Protocol number
      - aarp – AARP Ether Type (0x80F3)
      - appletalk – APPLETALK Ether Type (0x809B)
      - arp – ARP Ether Type (0x0806)
      - ip – IP Ether Type (0x0800)
      - ipv6 – IPv6 Ether Type (0x86DD)
      - ipx – IPX Ether Type (0x8137)
      - mint – MiNT Ether Type (0x8783)
      - rarp – RARP Ether Type (0x8035)
      - wisp – WISP Ether Type (0x8783)
    - vlan <1-4095> [log] rule-precedence <1-5000> rule-description <WORD> [type] – VLAN ID
      - <1-4095> – Specifies a VLAN ID from 1-4095

---

|                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>host&lt;dest-MAC&gt; &lt;AA-BB-CC-DD-EE-FF&gt; [dot1p &lt;0-7&gt;  log rule-precedence &lt;1-5000&gt;[rule-description &lt;WORD&gt; type [8021q &lt;1-65535&gt; aarp appletalk a rp ip ipv6 ipx mint rarp wisp] [log rule-precedence] vlan &lt;1-4095&gt; [log rule-precedence type[8021q &lt;1- 65535&gt; aarp appletalk arp ip ipv6 i px mint rarp wisp]</pre> | <pre>host - Specify an exact source MAC address to match</pre> <ul style="list-style-type: none"> <li>• &lt;dest-MAC&gt; - Specify the destination MAC address       <ul style="list-style-type: none"> <li>• dot1p &lt;0-7&gt; - Sets the 802.1p priority value from 0-7           <ul style="list-style-type: none"> <li>• log - Generates log messages when the packet coming from the interface matches an ACL entry. Log messages are generated only for router ACLs.</li> </ul> </li> <li>• rule-precedence&lt;1-5000&gt;rule-description &lt;WORD&gt; - Defines an integer value between 1-5000. This value sets the rule precedence in the ACL           <ul style="list-style-type: none"> <li>• &lt;1-5000&gt; - Specify a precedence value from 1-5000</li> <li>• rule-description - Access-list entry description</li> <li>• &lt;WORD&gt; - Enter the description not exceeding 128 characters</li> </ul> </li> </ul> </li> <li>• type[8021q &lt;1-65535&gt; aarp appletalk arp ip ipv6 ipx mint rarp wisp] [log &lt;0-7&gt; rule-precedence &lt;1-5000&gt;] - Specify the EtherType       <ul style="list-style-type: none"> <li>• 8021q - VLAN Ether Type (0x8100)</li> <li>• &lt;1-65535&gt; - Ethernet Protocol number</li> <li>• aarp - AARP Ether Type (0x80F3)</li> <li>• appletalk - APPLETALK Ether Type (0x809B)</li> <li>• arp - ARP Ether Type (0x0806)</li> <li>• ip - IP Ether Type (0x0800)</li> <li>• ipv6 - IPv6 Ether Type (0x86DD)</li> <li>• ipx - IPX Ether Type (0x8137)</li> <li>• mint - MINT Ether Type (0x8783)</li> <li>• rarp - RARP Ether Type (0x8035)</li> <li>• wisp - WISP Ether Type (0x8783)</li> </ul> </li> <li>• vlan &lt;1-4095&gt; [log rule-precedence &lt;1-5000&gt;rule-description &lt;WORD&gt; type - VLAN ID       <ul style="list-style-type: none"> <li>• &lt;1-4095&gt; - Specify a VLAN ID from 1-4095</li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### 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 takes 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/denied based on the ACLs configuration.

## Example

```
RFController(config-mac-acl-test)#deny 41-85-45-89-66-77 44-22-55-88-77-99
any vlan 1 log rule-precedence 2 rule-description test
RFController(config-mac-acl-test)#
```

The MAC ACL (in the example below) denies traffic from any source MAC address to a particular host MAC address:

```
RFController(config-mac-acl-test)#deny any host 00:01:ae:00:22:11
RFController(config-mac-acl-test)#
```

The example below denies traffic between two hosts based on MAC addresses:

```
RFController(config-mac-acl-test)#deny host 01:02:fe:45:76:89 host
01:02:89:78:78:45
RFController(config-mac-acl-test)#
```

## dhcp-server-policy

---

### In this chapter

- [dhcp-server-policy](#) ..... 638

This chapter summarizes the DHCP-Server-Policy commands within CLI structure.

Use the (config) instance to configure DHCP Server Policy related configuration commands. To navigate to the dhcp-server-policy instance, use the following commands:

```

RFController(config)#dhcp-server-policy <policy-name>
RFController(config)#dhcp-server-policy test
RFController(config-dhcp-server-policy-test)#
RFController(config-dhcp-policy-test)#?
DHCP policy Mode commands:
  bootp      BOOTP specific configuration
  dhcp-class  Configure DHCP Server class
  dhcp-pool   Configure DHCP server address pool
  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
RFController(config-dhcp-policy-test)#

```

## dhcp-server-policy

[Table 30](#) Summarizes dhcp-server-policy commands

**TABLE 30** dhcp-server-policy commands

| Command                    | Description                                     | Reference                |
|----------------------------|-------------------------------------------------|--------------------------|
| <a href="#">bootp</a>      | Configures a BOOTP specific configuration       | <a href="#">page 639</a> |
| <a href="#">dhcp-pool</a>  | Configures a DHCP server address pool           | <a href="#">page 640</a> |
| <a href="#">option</a>     | Defines the DHCP option used in DHCP pools      | <a href="#">page 674</a> |
| <a href="#">no</a>         | Negates a command or sets its default value     | <a href="#">page 675</a> |
| <a href="#">ping</a>       | Specifies ping parameters used by a DHCP server | <a href="#">page 676</a> |
| <a href="#">dhcp-class</a> | Configures a DHCP server class                  | <a href="#">page 677</a> |



## bootp

### *dhcp-server-policy*

Configures a BOOTP specific configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
bootp ignore
```

### Parameters

---

|              |                                                                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| bootp ignore | Configures a BOOTP specific configuration <ul style="list-style-type: none"><li>• ignore - Configures a DHCP server to ignore BOOTP requests</li></ul> |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-dhcp-policy-test)#bootp ignore
RFController(config-dhcp-policy-test)#
```

## dhcp-pool

### *dhcp-server-policy*

Configures a DHCP server address pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
RFController(config-dhcp-policy-test)#dhcp-pool pool1
RFController(config-dhcp-policy-test-pool-pool1)#
```

### Parameters

---

|        |                     |
|--------|---------------------|
| <WORD> | Specify a pool name |
|--------|---------------------|

---

### Example

```
RFController(config-dhcp-policy-test-pool-pool1)#?
DHCP pool Mode commands:
  address          Configure network pool's include address
  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
```

## dhcp-pool mode

Configures dhcp-pool commands

[Table 31](#) Summarizes dhcp-pool commands

**TABLE 31** dhcp-pool mode commands

| Command                             | Description                                                                                                                               | Reference                |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">address</a>             | Specifies a range of addresses for a DHCP network pool                                                                                    | <a href="#">page 641</a> |
| <a href="#">bootfile</a>            | Assigns a bootfile name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted | <a href="#">page 643</a> |
| <a href="#">ddns</a>                | Configures dynamic DNS parameters                                                                                                         | <a href="#">page 644</a> |
| <a href="#">default-router</a>      | Configures a default-router or gateway IP address for the network pool                                                                    | <a href="#">page 645</a> |
| <a href="#">dns-server</a>          | Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool                                                 | <a href="#">page 646</a> |
| <a href="#">domain-name</a>         | Sets the domain name for the network pool                                                                                                 | <a href="#">page 647</a> |
| <a href="#">excluded-address</a>    | Prevents a DHCP server from assigning certain addresses to the DHCP pool                                                                  | <a href="#">page 648</a> |
| <a href="#">lease</a>               | Sets a valid lease time for the IP address used by DHCP clients in the DHCP pool                                                          | <a href="#">page 649</a> |
| <a href="#">netbios-name-server</a> | Configures NetBIOS (WINS) name server IP address                                                                                          | <a href="#">page 651</a> |
| <a href="#">netbios-node-type</a>   | Defines the NetBIOS node type                                                                                                             | <a href="#">page 652</a> |
| <a href="#">next-server</a>         | Configures the next server in the boot process                                                                                            | <a href="#">page 653</a> |
| <a href="#">no</a>                  | Negates a command or sets its default value                                                                                               | <a href="#">page 654</a> |
| <a href="#">option</a>              | Configures RAW DHCP options                                                                                                               | <a href="#">page 655</a> |
| <a href="#">respond-via-unicast</a> | Sends a DHCP offer and a DHCP Ack as unicast messages                                                                                     | <a href="#">page 656</a> |
| <a href="#">update</a>              | Controls the usage of DDNS service                                                                                                        | <a href="#">page 657</a> |
| <a href="#">static-binding</a>      | Configures static address bindings                                                                                                        | <a href="#">page 660</a> |

## *address*

### *dhcp-pool mode commands*

Specifies a range of addresses for the DHCP network pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
address [address {class} <DHCP-CLASS>|range <Low IP> <High IP>{class}
<DHCP-CLASS>]
```

### **Parameters**

```
[address {class}
<DHCP-CLASS>|range <Low IP>
<High IP>{class} <DHCP-CLASS> ]
```

- address – Specify the address to include in the network pool
- range – Adds an address range for the DHCP server
  - <Low IP> – Defines the first IP address in the address range
  - <High IP> – Defines the last IP address in the address range

The following parameters are common for both the address and range

- class – Specify the DHCP class name to which the address range is attached
  - <DHCP-CLASS> – Specify the name of the DHCP class

### **Usage Guidelines**

Use the `no address range` command to remove the DHCP address range.

Use the `address` command to specify a range of addresses for the DHCP network pool. The DHCP server assigns IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address, and a low IP address is the lower limit for providing the IP address.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#address range 1.2.3.4
5.6.7.8 class dhcp1
RFController(config-dhcp-policy-test-pool-pool1)#
```

```
RFController(config-dhcp-policy-test-pool-pool1)#address 1.2.3.4 class dhcp1
RFController(config-dhcp-policy-test-pool-pool1)#
```

## *bootfile*

### *dhcp-pool mode commands*

Assigns a bootfile name for the DHCP configuration in the network pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
bootfile <WORD>
```

### **Parameters**

---

|        |                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <WORD> | Sets the boot image for BOOTP clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Usage Guidelines**

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients). Only one boot file is allowed per pool.

Use `{no} bootfile` command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command `[no]bootfile` removes the existing command from the pool.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#bootfile test.txt
RFController(config-dhcp-policy-test-pool-pool1)#
```

## *ddns*

### *dhcp-pool mode commands*

Configures dynamic DNS parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
ddns [domain-name <WORD>|multiple-userclass|server <A.B.C.D> {A.B.C.D}|ttl
<1-864000>]
```

### **Parameters**

|                            |                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| domain-name <WORD>         | Sets the domain name used for DDNS updates                                                                                                                                              |
| multiple-userclass         | Enables multiple user class option                                                                                                                                                      |
| server <A.B.C.D> {A.B.C.D} | Specify the server IP address to which DDNS updates have been sent <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; - Defines an IP address in dotted decimal format</li> </ul> |
| ttl <1-864000>             | Select a <i>Time To Live</i> (TTL) value between 1 and 864000 for DDNS updates                                                                                                          |

### **Usage Guidelines**

Use `update dns override` to enable an internal DHCP server to send DDNS updates for resource records (RRs) A, TXT and PTR. A DHCP server can always override the client even if the client is configured to perform the updates.

In the DHCP server network pool, FQDN is defined as the DDNS domain name. This is used internally in DHCP packets between the DHCP server on the controller and the DNS server.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#ddns domainname WID
RFController(config-dhcp-policy-test-pool-pool1)#

RFController(config-dhcp-policy-test-pool-pool1)#ddns multiple-user-class
RFController(config-dhcp-policy-test-pool-pool1)#

RFController(config-dhcp-policy-test-pool-pool1)#ddns server 172.16.10.9
RFController(config-dhcp-policy-test-pool-pool1)#
```

## *default-router*

### *dhcp-pool mode commands*

Configures a default-router or gateway IP address for the network pool. To remove the default router list, use the no default-router command.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
default-router <A.B.C.D> {<A.B.C.D>}
```

### **Parameters**

---

|                       |                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------|
| <A.B.C.D> {<A.B.C.D>} | Specifies the default router IP address for the network pool. The maximum number of IP's that can be configured is 8. |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------|

---

### **Usage Guidelines**

The IP address of the router should be on the same subnet as the client subnet.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#default-router 172.16.10.8  
172.16.10.9  
RFController(config-dhcp-policy-test-pool-pool1)#
```

## *dns-server*

### *dhcp-pool mode commands*

Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool. Use the no dns-server command to remove the DNS server list.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dns-server <A.B.C.D>
```

### **Parameters**

---

|                              |                                                                                                                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;A.B.C.D&gt;</code> | Configures the DNS server's IP address <ul style="list-style-type: none"> <li>• <code>&lt;A.B.C.D&gt;</code> – Sets the server's IP address. Up to 8 IPs can be set</li> </ul> |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Usage Guidelines**

For DHCP clients, 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.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#dns-server 172.16.10.7
RFController(config-dhcp-policy-test-pool-pool1)#
```



## *domain-name*

### *dhcp-pool mode commands*

Sets the domain name for the DHCP pool. Use the `no domain-name` command to remove the domain name.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
domain-name <WORD>
```

### **Parameters**

---

|        |                                           |
|--------|-------------------------------------------|
| <WORD> | Defines the domain name for the DHCP pool |
|--------|-------------------------------------------|

---

### **Usage Guidelines**

For DHCP clients, 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.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#domain-name documentation
RFController(config-dhcp-policy-test-pool-pool1)#
```

***excluded-address****dhcp-pool mode commands*

Prevents a DHCP Server from assigning certain addresses to the DHCP pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
excluded-address [ <A.B.C.D> | range <Low IP> <High IP> ]
```

**Parameters**

[ <A.B.C.D> | range <Low IP>  
<High IP> ]

- <A.B.C.D> – Specify the IP address to exclude or low IP address in a range
- range – Specify a range of excluded addresses from the DHCP pool
- <Low IP> – Specify the low IP address to exclude
- <High IP> – Specify the high IP address to exclude

These IP addresses are excluded by the DHCP server when assigning IP address to servers

**Example**

```
RFController(config-dhcp-policy-test)#excluded-address 172.16.10.9
172.16.10.10
RFController(config-dhcp-policy-test)#
```

## *lease*

### *dhcp-pool mode commands*

Sets a valid lease time for the IP address used by DHCP clients in the DHCP pool

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
lease [<0-365> {0-23} {0-59} {0-59}|infinite]
```

### **Parameters**

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <0-365>  | <p>Select a value between 0 and 365 days to configure lease time. Days may be 0 only when hours and/or mins are greater than 0</p> <ul style="list-style-type: none"> <li>• &lt;0-23&gt; – Sets the lease period in hours. Hours can be 0 only when days and/or minutes are configured with a value greater than 0</li> <li>• &lt;0-59&gt; – Sets the lease period in minutes. Minutes can be 0 only when days and/or hours are configured with a value greater than 0</li> <li>• &lt;0-59&gt; – Sets the lease period in seconds</li> </ul> |
| infinite | Sets the the lease time as infinite                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### **Usage Guidelines**

If lease parameter is not configured on the DHCP pool, the default value is used. The default value of the lease is 24 hours.

**Example**

```

RFController(config-dhcp-policy-test-pool-pool1)#lease 1 0 0
RFController(config-dhcp-policy-test-pool-pool1)#

RFController(config-dhcp-policy-test-pool-pool1)# show running-config
include-factory
.....
ip dhcp pool Test4lease
  lease 1 0 0
  no domain-name
  no bootfile
  no dns-server
  no default-router
  no next-server
  no netbios-name-server
  no netbios-node-type
  no unicast-enable
  no update dns
  no ddns domainname
  no ddns ttl
  no ddns multiple-user-class
  client-name test4lease
  client-identifier tested4lease
.....
RFController(config-dhcp-policy-test-pool-pool1))#

RFController(config-dhcp-policy-test-pool-pool1)#lease infinite
RFController(config-dhcp-policy-test-pool-pool1)#

```

## *netbios-name-server*

### *dhcp-pool mode commands*

Configures the NetBIOS (WINS) name server IP address

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
netbios-name-server <A.B.C.D>
```

### **Parameters**

---

|           |                                           |
|-----------|-------------------------------------------|
| <A.B.C.D> | Sets the NetBIOS name server's IP address |
|-----------|-------------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#netbios-name-server  
172.16.10.23  
RFController(config-dhcp-policy-test-pool-pool1)#
```

***netbios-node-type****dhcp-pool mode commands*

Defines the netbios-node-type

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
netbios-node-type [b-node|h-mode|m-node|p-node]
```

**Parameters**


---

|                                   |                                                                                                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [b-node h-mode <br>m-node p-node] | Defines the netbios-node-type <ul style="list-style-type: none"> <li>• b-node – The type is broadcast node</li> <li>• h-node – The type is hybrid node</li> <li>• m-node – The type is mixed node</li> <li>• p-node – The type is peer-to-peer node</li> </ul> |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#netbios-node-type
b-node
RFController(config-dhcp-policy-test-pool-pool1)#
```

## *next-server*

### *dhcp-pool mode commands*

Configures the next-server in the boot process

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
next-server <A.B.C.D>
```

### **Parameters**

---

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| <A.B.C.D> | Configures the IP address of the next-server in the boot process |
|-----------|------------------------------------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#next-server 172.16.10.24  
RFController(config-dhcp-policy-test-pool-pool1)#
```

**no***dhcp-pool mode commands*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**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]
```

**Parameters**


---

|                                   |                                                                      |
|-----------------------------------|----------------------------------------------------------------------|
| [address bootfile ddns            | • address – Unconfigures network pool's include addresses            |
| default-router dns-server domain- | • bootfile – Specifies a boot file name                              |
| name excluded-address             | • default-router – Unconfigures the default router                   |
| lease netbios-name-server netbio  | • dns-server – Unconfigures the DNS server                           |
| s-node-type network               | • domain-name – Unconfigures the domain name                         |
| next-server option respond-via-un | • excluded-address – Prevents a DHCP server from assigning certain   |
| icast                             | addresses                                                            |
| static-binding                    | • lease – Disables an address lease time                             |
| static-route update]              | • netbios-name-server – Unconfigures NetBIOS (WINS) name server      |
|                                   | • netbios-node-type – Unconfigures NetBIOS node type                 |
|                                   | • next-server – Unconfigures the next server in the boot process     |
|                                   | • option – Raw DHCP options                                          |
|                                   | • respond-via-unicast – Sends a DHCP offer and DHCP Ack as broadcast |
|                                   | messages                                                             |
|                                   | • static-binding – Removes static address bindings                   |
|                                   | • static-route – Adds static routes installed on DHCP clients        |
|                                   | • update – Controls the usage of DDNS service                        |

---

**Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#no bootfile
RFController(config-dhcp-policy-test-pool-pool1)#

RFController(config-dhcp-policy-test-pool-pool1)#no network
RFController(config-dhcp-policy-test-pool-pool1)#

RFController(config-dhcp-policy-test-pool-pool1)#no lease
RFController(config-dhcp-policy-test-pool-pool1)#

RFController(config-dhcp-policy-test-pool-pool1)#no default-router
RFController(config-dhcp-policy-test-pool-pool1)#
```



## *option*

### *dhcp-pool mode commands*

Configures raw DHCP options. The DHCP option has to be configured under the DHCP-Server-Policy. The options configured under the DHCP-Pool/DHCP-Server-Policy can also be used in static-binding.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
option <option-name> [<A.B.C.D>|<WORD>]
```

### **Parameters**

|               |                                                  |
|---------------|--------------------------------------------------|
| <option-name> | Specify the name of the DHCP option to configure |
| <A.B.C.D>     | Sets the IP value of the DHCP option             |
| <WORD>        | Sets the ASCII value of the DHCP option          |

### **Usage Guidelines**

Defines non standard DHCP option codes (0-254)

### **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**

```
RFController(config-dhcp-policy-test-pool-pool1)#option option1
157.235.208.80
RFController(config-dhcp-policy-test-pool-pool1)#
```

## *respond-via-unicast*

### *dhcp-pool mode commands*

Sends DHCP offer and DHCP Ack as unicast messages

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
respond-via-unicast
```

### **Parameters**

None

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#respond-via-unicast  
RFController(config-dhcp-policy-test-pool-pool1)#
```

---

### **NOTE**

The commands `clear`, `commit`, `exit`, `help`, `show`, `service`, `revert`, `write` are common commands. Refer to [Chapter 6, Common Commands](#) for more information.

---

## *update*

### *dhcp-pool mode commands*

Controls the usage of the DDNS service

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
update dns {override}
```

### **Parameters**

---

|                |                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------|
| dns {override} | Dynamic DNS Configuration                                                                                     |
|                | <ul style="list-style-type: none"> <li>• override – Enables dynamic updates by onboard DHCP Server</li> </ul> |

---

### **Usage Guidelines**

A DHCP client cannot perform updates for RR's A, TXT and PTR. Use `update (dns)(override)` to enable the controller's internal DHCP server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can override the client, even if the client is configured to perform the updates.

In the DHCP pool of DHCP server, FQDN is configured as the DDNS domain name. This is used internally in DHCP packets between the controller's DHCP server and the DNS server.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1)#update dns override
RFController(config-dhcp-policy-test-pool-pool1)#
```

## static-binding

### *dhcp-pool mode commands*

Configures static address bindings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
static-binding [client-identifier <WORD>|hardware-address
<AA-BB-CC-DD-EE-FF>]
```

### Parameters

---

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [client-identifier<br><WORD> hardware-address<br><AA-BB-CC-DD-EE-FF>] | <ul style="list-style-type: none"> <li>• client-identifier &lt;WORD&gt; - Specify the client identifier for the DHCP client (DHCP option 61) <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - ASCII string. To prepend null character use \\0 at beginning. Single \ in the input will be ignored.</li> </ul> </li> <li>• hardware-address &lt;AA-BB-CC-DD-EE-FF&gt; - Specify the hardware address of the DHCP client</li> </ul> |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFCcontroller(config-dhcp-policy-test-pool-pool1)#static-binding
client-identifier Hex
RFCcontroller(config-dhcp-policy-test-pool-pool1-binding-Hex)#?
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

```

```
RFController(config-dhcp-policy-test-pool-pool1-binding-Hex)#
```

```
RFController(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

```

```
RFController(config-dhcp-policy-test-pool-pool1-binding-11-22-33-44-55-66)#
```

## static-binding mode

Use the (config) instance to configure `dhcp-static-binding` related configuration commands. To navigate to the instance, use the following commands:

```
rRFController(config-dhcp-policy-test-pool-pool1)#static-binding
client-identifier Hex
RFController(config-dhcp-policy-test-pool-pool1-binding-Hex)#?
```

[Table 32](#) Summarizes static-binding-mode commands

**TABLE 32** static-binding mode

| Command                             | Description                                                                               | Reference                |
|-------------------------------------|-------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">bootfile</a>            | Assigns a bootfile name for the DHCP configuration on the network pool                    | <a href="#">page 661</a> |
| <a href="#">client-name</a>         | Specifies a client-name to configure                                                      | <a href="#">page 662</a> |
| <a href="#">default-router</a>      | Configures default-router or gateway IP address for the network pool                      | <a href="#">page 663</a> |
| <a href="#">dns-server</a>          | Sets the DNS server's IP address available to all DHCP clients connected to the DHCP pool | <a href="#">page 664</a> |
| <a href="#">domain-name</a>         | Sets the domain name for the network pool                                                 | <a href="#">page 665</a> |
| <a href="#">ip-address</a>          | Configures a fixed IP address for a host                                                  | <a href="#">page 666</a> |
| <a href="#">netbios-name-server</a> | Configures a NetBIOS (WINS) name server IP address                                        | <a href="#">page 667</a> |
| <a href="#">netbios-node-type</a>   | Defines the NetBIOS node type                                                             | <a href="#">page 668</a> |
| <a href="#">next-server</a>         | Configures the next-server in the boot process                                            | <a href="#">page 669</a> |
| <a href="#">no</a>                  | Negates a command or sets its default value                                               | <a href="#">page 670</a> |
| <a href="#">option</a>              | Configures raw DHCP options                                                               | <a href="#">page 671</a> |
| <a href="#">respond-via-unicast</a> | Sends a DHCP offer and DHCP Ack as unicast messages                                       | <a href="#">page 656</a> |
| <a href="#">static-route</a>        | Adds static routes to be installed on DHCP clients                                        | <a href="#">page 673</a> |

## *bootfile*

### *static-binding mode*

Specifies a bootfile name for the DHCP configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
bootfile <WORD>
```

### **Parameters**

---

|        |                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <WORD> | Specify a boot file name. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted. |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|

---

### **Usage Guidelines**

Use the bootfile command to specify the boot image. The boot file contains the boot image name used for booting the BOOTP clients (DHCP clients). Only one boot file is allowed per pool.

Use {no} bootfile command to remove the bootfile. Do not use the <file name> with the bootfile command as only one bootfile exists per pool. The command [no] bootfile removes the existing command from the pool.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#bootfile test.txt
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```

## *client-name*

### *static-binding mode*

Specifies a client-name to configure

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
client-name <WORD>
```

### **Parameters**

---

|        |                                    |
|--------|------------------------------------|
| <WORD> | Specify a client-name to configure |
|--------|------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#client-name RFID  
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```



## *default-router*

### *static-binding mode*

Configures the default router or gateway IP address for the network pool. To remove the default router list, use the no default-router command.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
default-router <A.B.C.D> {A.B.C.D}
```

### **Parameters**

---

|                     |                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| <A.B.C.D> {A.B.C.D} | Specify an IP address to configure a default router. The maximum number of IPs that can be configured is 8. |
|---------------------|-------------------------------------------------------------------------------------------------------------|

---

### **Usage Guidelines**

The IP address of the router should be on the same subnet as the client subnet.

### **Example**

```
RFController(config-dhcp-net-pool-test)#default-router 157.235.208.246
157.235.208.247
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#show context
network-pool nw
default-router 157.235.208.246 157.235.208.247
```

***dns-server******static-binding mode***

Sets the DNS server's IP address available to all DHCP clients connected to the pool. Use the no dns-server command to remove the DNS server list.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
dns-server <A.B.C.D>
```

**Parameters**


---

|                              |                                                                                |
|------------------------------|--------------------------------------------------------------------------------|
| <code>&lt;A.B.C.D&gt;</code> | Specify a static IP address to configure a DNS server. Up to 8 IPs can be set. |
|------------------------------|--------------------------------------------------------------------------------|

---

**Usage Guidelines**

For DHCP clients, the DNS server's IP address maps the host name to an IP address. DHCP clients use the DNS server's IP address based in the order (sequence) configured.

**Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#dns-server
172.16.10.7
RFController(config-dhcp-net-pool-test)#
```

## *domain-name*

### *static-binding mode*

Configures a domain name

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
domain-name <WORD>
```

### **Parameters**

---

|        |                               |
|--------|-------------------------------|
| <WORD> | Specify a name for the domain |
|--------|-------------------------------|

---

### **Usage Guidelines**

The domain name cannot exceed 256 characters.

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#domain-name  
Technicaldocumentation  
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```

## *ip-address*

### *static-binding mode*

Configures a fixed IP address for a host

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
ip-address <A.B.C.D>
```

### **Parameters**

---

|           |                                                                     |
|-----------|---------------------------------------------------------------------|
| <A.B.C.D> | Configures a fixed IP address in dotted decimal format for the host |
|-----------|---------------------------------------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#ip-address  
172.16.10.9  
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```

## *netbios-name-server*

### *static-binding mode*

Configures a NetBIOS (WINS) name server's IP address

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
netbios-name-server <A.B.C.D>
```

### **Parameters**

---

|           |                                           |
|-----------|-------------------------------------------|
| <A.B.C.D> | Sets the NetBIOS name server's IP address |
|-----------|-------------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#netbios-name-server 172.16.10.27
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```

***netbios-node-type******static-binding mode***

Assigns a the netbios-node-type from the list

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
netbios-node-type [b-node|h-mode|m-node|p-node]
```

**Parameters**


---

|                                   |                                                                                                                                                                                                                                                                                        |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [b-node h-mode <br>m-node p-node] | Defines the NetBIOS (WINS) name servers from the list <ul style="list-style-type: none"> <li>• b-node – The type is broadcast node</li> <li>• h-node – The type is hybrid node</li> <li>• m-node – The type is mixed node</li> <li>• p-node – The type is peer-to-peer node</li> </ul> |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#netbios-node-type
p-node
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```

## *next-server*

### *static-binding mode*

Configures the next-server in the boot process

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
next-server <A.B.C.D>
```

### **Parameters**

---

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| <A.B.C.D> | Configures the IP address of the next-server in the boot process |
|-----------|------------------------------------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#next-server  
172.16.10.30  
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#
```

**no****static-binding mode**

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**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]
```

**Parameters**


---

|                                                              |                                                                               |
|--------------------------------------------------------------|-------------------------------------------------------------------------------|
| [bootfile client-name default-router dns-server              | • bootfile – Specifies a boot file name                                       |
| domain-name ip-address netbios-name-server netbios-node-type | • client-name – Removes a client-name                                         |
| next-server option respond-via-unicast static-route]         | • default-router – Configures a default router                                |
|                                                              | • dns-server – Configures a DNS server                                        |
|                                                              | • domain-name – Configures a domain name                                      |
|                                                              | • ip-address – Disables a fixed IP address for the host                       |
|                                                              | • netbios-name-server – Configures a NetBIOS (WINS) name server               |
|                                                              | • netbios-node-type – Configures a NetBIOS node type                          |
|                                                              | • next-server – Configures a next server in boot process                      |
|                                                              | • option – Raw DHCP options                                                   |
|                                                              | • respond-via-unicast – Sends a DHCP offer and DHCP Ack as broadcast messages |
|                                                              | • static-route – Removes static routes installed on DHCP clients              |

---

**Example**

```
RFController(config-dhcp-net-pool-test)#no bootfile
RFController(config-dhcp-net-pool-test)#
```



## *option*

### *static-binding mode*

Configures raw DHCP options. The DHCP option has to be configured under DHCP-Policy. The options configured under DHCP-Server-Policy only can be used in static-binding.

```
RFController(config-dhcp-policy-test)#option test1 2 ascii
RFController(config-dhcp-policy-test)#
```

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
option [<A.B.C.D> | <WORD>]
```

### **Parameters**

|           |                                         |
|-----------|-----------------------------------------|
| <A.B.C.D> | Sets the IP value of the DHCP option    |
| <WORD>    | Sets the ASCII value of the DHCP option |

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-ascii)#option option1
172.16.10.10
RFController(config-dhcp-policy-test-pool-pool1-binding-ascii)#
```

## *respond-via-unicast*

### *static-binding mode*

Sends a DHCP offer and DHCP Acknowledge as unicast messages

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
respond-via-unicast
```

### **Parameters**

None

### **Example**

```
RFController(config-dhcp-net-pool-test)#respond-via-unicast  
RFController(config-dhcp-net-pool-test)#
```

## *static-route*

### *static-binding mode*

Adds static routes to be installed on the DHCP clients

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
static-route <A.B.C.D/M> <A.B.C.D>
```

### **Parameters**

---

|             |                                                           |
|-------------|-----------------------------------------------------------|
| <A.B.C.D/M> | Enter the network number and mask to configure the subnet |
|-------------|-----------------------------------------------------------|

---

### **Example**

```
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#static-route  
10.0.0.0/10 157.235.208.235  
RFController(config-dhcp-policy-test-pool-pool1-binding-1)#?
```

### **NOTE**

The commands `clear`, `commit`, `exit`, `help`, `write`, `revert`, `service` and `show` are common commands. For more information, see [Chapter 6, Common Commands](#).

---

## option

### *dhcp-server-policy*

Defines the DHCP option used in DHCP pools

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
option <WORD> <0-254> [ascii|ip]
```

### Parameters

---

|                                         |                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;WORD&gt; &lt;0-254&gt;</code> | <p>Sets raw DHCP options</p> <ul style="list-style-type: none"> <li>• <code>&lt;0-254&gt;</code> – Enter an option code between 0 and 254             <ul style="list-style-type: none"> <li>• <code>ascii</code> – Sets the ASCII value of the DHCP option</li> <li>• <code>ip</code> – Sets the IP value of the DHCP option</li> </ul> </li> </ul> |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Usage Guidelines

Defines non standard DHCP option codes (0-254)

### 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

```
RFController(config-dhcp-policy-test)#option test1 2 ascii
RFController(config-dhcp-policy-test)#

RFController(config-dhcp-policy-test)#option test1 2 ip
RFController(config-dhcp-policy-test)#
```

## no

### *dhcp-server-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [bootp|excluded-address|host-pool|network-pool|option|ping]
```

### Parameters

---

|                  |                                                                              |
|------------------|------------------------------------------------------------------------------|
| [bootp]          | • bootp – Unconfigures BOOTP specific configuration                          |
| excluded-address | • excluded-address – Prevents a DHCP server from assigning certain addresses |
| host-pool        | • host-pool – Deletes the DHCP server host address pool                      |
| network-pool     | • network-pool – Deletes the DHCP server address pool                        |
| option ping]     | • option – Removes the DHCP server option                                    |
|                  | • ping – Specifies default ping parameters used by a DHCP Server             |

---

### Example

```
RFController(config-dhcp-policy-test)#no bootp ignore
RFController(config-dhcp-policy-test)#

RFController(config-dhcp-policy-test)#no option test1
RFController(config-dhcp-policy-test)#
```

## ping

### *dhcp-server-policy*

Specifies ping parameters used by a DHCP Server

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ping timeout <1-10>
```

### Parameters

---

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| timeout <1-10> | Select a value between 1 and 10 to specify the ping timeout (in seconds) |
|----------------|--------------------------------------------------------------------------|

---

### Example

```
RFController(config-dhcp-policy-test)#ping timeout 2
RFController(config-dhcp-policy-test)#
```

## dhcp-class

### *dhcp-server-policy*

Configures DHCP Server class

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
dhcp-class <DHCP-CLASS>
```

### Parameters

---

|                                 |                           |
|---------------------------------|---------------------------|
| <code>&lt;DHCP-CLASS&gt;</code> | Specify a DHCP class name |
|---------------------------------|---------------------------|

---

### Example

```
RFController(config-dhcp-policy-test)#dhcp-class dhcpclass1
RFController(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
```

## dhcp-class mode

Use the (config-dhcpclass) instance to configure DHCP user classes. The controller supports a maximum of 8 user classes per DHCP class. To navigate to this instance use the command:

```
RFController(config-dhcp-policy-test)#dhcp-class dhcpclass1
RFController(config-dhcp-policy-test-class-dhcpclass1)#?
```

Table 33 Summarizes dhcp-class commands

**TABLE 33** dhcp-class mode commands

| Command                    | Description                                 | Reference                |
|----------------------------|---------------------------------------------|--------------------------|
| <i>multiple-user-class</i> | Enables multiple user class option          | <a href="#">page 679</a> |
| <i>no</i>                  | Negates a command or sets its default value | <a href="#">page 680</a> |
| <i>option</i>              | Configures DHCP server options              | <a href="#">page 681</a> |



## *multiple-user-class*

### *dhcp-class mode commands*

Enables multiple user class option

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
multiple-user-class
```

### **Parameters**

None

### **Example**

```
RFController(config-dhcp-policy-test-class-class1)#multiple-user-class  
RFController(config-dhcp-policy-test-class-class1)#
```

*no*

*dhcp-class mode commands*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [multiple-user-class|option]
```

### Parameters

- 
- |                              |                                                                                                                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [multiple-user-class option] | <ul style="list-style-type: none"><li>• multiple-user-class – Disables the multiple user class option</li><li>• option – Unconfigures (removed updates for) DHCP server options</li></ul> |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

### Example

```
RFController(config-dhcp-policy-test-class-class1)#no multiple-user-class  
RFController(config-dhcp-policy-test-class-class1)#
```

## *option*

### *dhcp-class mode commands*

Configures DHCP server options

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
option user-class <WORD>
```

### **Parameters**

- 
- |                    |                                                                   |
|--------------------|-------------------------------------------------------------------|
| user-class [<WORD> | • user-class - Configures DHCP server user-class options          |
|                    | • <WORD> - Sets the ASCII value of user-class option to configure |
- 

### **Example**

```
RFController(config-dhcp-policy-test-class-class1)#option user-class hex  
RFController(config-dhcp-policy-test-class-class1)#
```



# firewall-policy

---

## In this chapter

- [firewall-policy . . . . . 684](#)

This chapter summarizes the firewall-policy commands within the CLI structure.

Use (config) instance to configure firewall-policy related configuration commands. To navigate to the config-fw-policy instance, use the following commands.

```

RFController(config)#firewall-policy <policy-name>
RFController(config)#firewall-policy test
RFController(config-fw-policy-test)#?
Firewall policy Mode commands:
  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
  logging                           Firewall enhanced logging
  no                                 Negate a command or set its defaults
  proxy-arp                          Enable generation of ARP responses 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

RFController(config-fw-policy-test)#

```

## firewall-policy

Table 34 Summarizes default firewall policy commands

**TABLE 34** firewall-policy commands

| Command                              | Description                                                                 | Reference                   |
|--------------------------------------|-----------------------------------------------------------------------------|-----------------------------|
| <i>alg</i>                           | Enables an algorithm                                                        | <a href="#">page 685</a>    |
| <i>clamp</i>                         | Sets a clamp value to limit TCP MSS to inner path-MTU for tunnelled packets | <a href="#">page 686</a>    |
| <i>dhcp-offer-convert</i>            | Enables the conversion of broadcast DHCP offers to unicast                  | <a href="#">page 687</a>    |
| <i>dns-snoop</i>                     | Sets the timeout value for DNS entries                                      | <a href="#">page 688</a>    |
| <i>firewall</i>                      | Configures the wireless firewall                                            | <a href="#">page 689</a>    |
| <i>flow</i>                          | Defines a session flow timeout                                              | <a href="#">page 15-690</a> |
| <i>ip</i>                            | Configures IP for a selected component                                      | <a href="#">page 692</a>    |
| <i>ip-mac</i>                        | Defines an action based on IP-MAC table                                     | <a href="#">page 695</a>    |
| <i>logging</i>                       | Enables enhanced firewall logging                                           | <a href="#">page 696</a>    |
| <i>no</i>                            | Negates a command or sets its default value                                 | <a href="#">page 697</a>    |
| <i>proxy-arp</i>                     | Enables the generation of ARP responses on behalf of another device         | <a href="#">page 698</a>    |
| <i>stateful-packet-inspection-12</i> | Enables stateful-packets-inspection in layer2 firewall                      | <a href="#">page 15-699</a> |
| <i>storm-control</i>                 | Defines storm-control and sets logging                                      | <a href="#">page 700</a>    |
| <i>virtual-defragmentation</i>       | Enables virtual defragmentation for IPv4 packets                            | <a href="#">page 702</a>    |

## alg

### *firewall-policy*

Enables a selected algorithm

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
alg [dns|ftp|sip|tftp]
```

### Parameters

---

|                                   |                                                                                                                                                                           |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [dns ftp h323 http sccp sip tftp] | Enables selected algorithm from the list                                                                                                                                  |
|                                   | <ul style="list-style-type: none"><li>• dns - Enables DNS ALG</li><li>• ftp - Enables FTP ALG</li><li>• sip - Enables SIP ALG</li><li>• tftp - Enables TFTP ALG</li></ul> |

---

### Example

```
RFController(config-fw-policy-default)# alg tftp
RFController(config-fw-policy-default)#
```

## clamp

### *firewall-policy*

Sets the clamp value used to limit TCP MSS to inner path-MTU for tunnelled packets

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
clamp tcp-mss
```

### Parameters

---

|         |                                                                                    |
|---------|------------------------------------------------------------------------------------|
| tcp-mss | Sets the clamp value used to limit TCP MSS to inner path-MTU for tunnelled packets |
|---------|------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-fw-policy-test)#clamp tcp-mss  
RFController(config-fw-policy-test)#
```



## dhcp-offer-convert

### *firewall-policy*

Enables the conversion of broadcast DHCP offers to unicast

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dhcp-offer-convert
```

### **Parameters**

None

### **Example**

```
RFController(config-fw-policy-default)#dhcp-offer-convert  
RFController(config-fw-policy-default)#
```

## dns-snoop

### *firewall-policy*

Sets the timeout value for DNS entries

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
dns-snoop entry-timeout <30-86400>
```

### Parameters

---

|                          |                                                                     |
|--------------------------|---------------------------------------------------------------------|
| entry-timeout <30-86400> | Sets the timeout value for DNS entries between 30 and 86400 seconds |
|--------------------------|---------------------------------------------------------------------|

---

### Example

```
RFController(config-fw-policy-test)#dns-snoop entry-timeout 35
RFController(config-fw-policy-test)#
```

## firewall

### *firewall-policy*

Configures the wireless firewall

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
firewall enable
```

### Parameters

---

|                 |                               |
|-----------------|-------------------------------|
| firewall enable | Enables the wireless firewall |
|-----------------|-------------------------------|

---

### Example

```
RFController(config-fw-policy-default)#firewall enable
RFController(config-fw-policy-default)#
```

## flow

### *firewall-policy*

Defines the session flow timeout for different packet types

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
flow [dhcp|timeout]
flow dhcp stateful
flow timeout [icmp|other|tcp|udp]
flow timeout [icmp|other|udp] <1-32400>
flow timeout tcp [close-wait|reset|setup|stateless-fin-or-reset|
stateless-general] <1-32400>
flow timeout tcp established <15-32400>
```

**Parameters**


---

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [dhcp timeout] | <p>Defines session flow timeout</p> <ul style="list-style-type: none"> <li>• dhcp stateful – Sets the DHCP flow between 1 and 32400 seconds</li> <li>• timeout [icmp other udp] &lt;1-32400&gt; – Sets the flow timeout based on the packet type <ul style="list-style-type: none"> <li>• icmp – Sets the timeout for ICMP packets between 1 and 32400 seconds</li> <li>• other – Sets the timeout for any packet type between 1 and 32400 seconds</li> <li>• udp &lt;1-32400&gt; – Sets the timeout for UDP packets between 1 and 32400 seconds <ul style="list-style-type: none"> <li>• &lt;1-32400&gt; – Based on the packet type, the timeout is set between 1 and 32400 seconds</li> </ul> </li> </ul> </li> <li>• tcp[close-wait established reset setup stateless-fin-or-reset stateless-general ] – Based on the TCP state, the timeout is set between 1 and 32400 seconds] <ul style="list-style-type: none"> <li>• close-wait &lt;1-32400&gt; – Closed TCP flow</li> <li>• established &lt;15-32400&gt; – Established TCP flow. Set the timeout between 15 and 32400 seconds</li> <li>• reset &lt;1-32400&gt; – Reset TCP flow</li> <li>• setup &lt;1-32400&gt; – Opening TCP flow</li> <li>• stateless-fin-or-reset &lt;1-32400&gt; – Stateless TCP flow created with FIN or RESET packet</li> <li>• stateless-general &lt;1-32400&gt; – Stateless TCP Flow <ul style="list-style-type: none"> <li>• &lt;1-32400&gt; – Based on the packet type, the timeout is set between 1 and 32400 seconds</li> </ul> </li> </ul> </li> </ul> |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```

RFController(config-fw-policy-default)#flow timeout icmp 4
RFController(config-fw-policy-default)#

RFController(config-fw-policy-default)#flow timeout tcp setup 8
RFController(config-fw-policy-default)#

RFController(config-fw-policy-default)#flow icmp stateful
RFController(config-fw-policy-default)#

```

## ip

### *firewall-policy*

Configures a selected *Internet Protocol* (IP) component

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```

ip [dos|tcp]
ip dos {ascend/broadcast-multicast-icmp/chargen/fraggle/
      ftp-bounce/invalid-protocol/ip-ttl-zero/ipspoof/land/option-route/
      router-solicit/router-advt/smurf/snork/tcp-bad-sequence/tcp-fin-scan/
      tcp-intercept/tcp-max-incomplete/tcp-null-scan | tcp-post-syn |
      tcp-xmas-scan |tcphdrfrag |twinge/udp-short-hdr} [drop-only|
      log-and-drop|log-only]

ip dos {ascend/broadcast-multicast-icmp/chargen/fraggle/
      ftp-bounce/invalid-protocol/ip-ttl-zero/ipspoof/land/option-route/
      router-solicit/router-advt/smurf/snork/tcp-bad-sequence/tcp-fin-scan/
      tcp-intercept/| tcp-null-scan | tcp-post-syn |
      tcp-xmas-scan |tcphdrfrag |twinge/udp-short-hdr/winnuke} [log-and-drop|
      log-only] log-level [<0-8>|alerts|critical|debugging|emergencies|error|
      informational|none|notifications|warnings]
ip dos {tcp-max-incomplete [high/low] <1-1000>}

ip tcp [adjust-mss <472-1460>|optimize-unnecessary-resends|
      recreate-flow-on-out-of-state-syn|validate-icmp-unreachable|
      validate-rst-ack-number|validate-rst-seq-number]

```

**Parameters**

---

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>dos {ascend  <br/>         bcast-mcast-icmp<br/>          chargen  fraggle  </p> <p>ftp-bounce  invalid-protocol  <br/>         ip-ttl-zero  ipspooof  land  <br/>         option-route  <br/>         router-solicit  router-advt  <br/>         smurf  snork  tcp-bad-sequence  t<br/>         cp-fin-scan  <br/>         tcp-intercept  tcp-max-incomplete  <br/>         tcp-null-scan  <br/>         tcp-post-syn  <br/>         tcp-xmas-scan  tcp-hdrfrag<br/>          twinge  udp-short-hdr<br/>         [drop-only  log-and-drop  <br/>         log-only  log-level [&lt;0-8&gt;  <br/>         alerts  critical  debugging  <br/>          emergencies  <br/>         errors  informational  none  notific<br/>         ations  <br/>         warnings]</p> | <p>Configures the <i>Denial of Service</i> (DOS) attack parameter</p> <ul style="list-style-type: none"> <li>• ascend – Enables ascend DoS checks</li> <li>• bcast-mcast-icmp – Detects broadcast/multicast Icmp traffic as attack</li> <li>• chargen – Enables chargen DoS checks</li> <li>• fraggle – Enables fraggle DoS checks</li> <li>• ftp-bounce – Enables FTP bounce logs and sets the logging levels</li> <li>• invalid-protocol – Enables an invalid protocol DoS attack check and sets the logging levels for this attack</li> <li>• ip-ttl-zero – Enables a TCP IP TTL ZERO DoS attack check</li> <li>• ipspooof – Enables an IPSPOOF DoS attack check</li> <li>• land – Enables a LAND DoS attack check</li> <li>• option-route – Enables IP option route check</li> <li>• router-advt – Enables an ICMP router advertisement check</li> <li>• router-solicit – Enables an ICMP router solicit check</li> <li>• smurf log – Enables a smurf attack check</li> <li>• snork – Enables a packet check</li> <li>• tcp-intercept – Enables a TCP intercept</li> <li>• tcp-bad-sequence – Enables a TCP BAD SEQUENCE DoS attack check</li> <li>• tcp-fin-scan – Enables a TCP FIN SCAN DoS attack check</li> </ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

- tcp-null-scan – Enables a TCP NULL SCAN DoS attack check
- tcp-post-syn – Enables a TCP Post Syn DoS attack check
- tcp-xmas-scan – Enables a TCP XMAS SCAN DoS attack check
- tcp-hdrfrag – Enables Ta CP Header Fragm
- twinge – Enables a twinge check
- udp-short-hdr – Enables a UDP shortheadheader DoS attack check
- winnuke – Enables WINNUKE DoS attack

For all the above, the following parameters are common:

- drop-only – Drops the packet only
- log-and-drop log-level – Logs the details and drops the packet
- log-only log-level – Logs the details only
  - log-level [<0-8> |alerts |critical |debugging |  
 |emergencies |errors |  
 informational |none |notifications |warnings] – Configures the log level for a DoS check

---

For all the above DoS attacks, the following log-levels can be set

- alerts – Immediate action needed (level 1)
- critical – Critical conditions (level 2)
- <0-8> – Select one numerical log level. All messages with and below this severity are logged
- emergencies – System is unusable (level 0)
- errors – Error conditions (level 3)
- warnings – Warning conditions (level 4)
- notifications – Normal but significant conditions (level 5)
- informational – Informational messages (level 6)
- debugging – Debugging messages (level 7)
- none – Disable logging (level 8)
- tcp-max-incomplete – Configures the maximum half-open TCP connections in the system
  - high <1-1000> – Sets the upper threshold value between 1 and 1000
  - low <1-1000> – Sets the lower threshold value between 1 and 1000

---

```
tcp [adjust-mss <472-1460> |
optimize-unnecessary-resends |
recreate-flow-on-out-of-state-syn |
validate-icmp-unreachable |
validate-rst-ack-number |
validate-rst-seq-number]
```

Configures TCP protocol settings

- adjust-mss <472-1460> – Sets TCP MSS adjustment value
    - <472-1460> – Sets the maximum value of TCP MSS option (472-1460)
  - optimize-unnecessary-resends – Enables checking of unnecessary resend of TCP packets
  - recreate-flow-on-out-of-state-syn – Allows a 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 checking of sequence number in ICMP unreachable error packets which aborts an established TCP flow
  - validate-rst-ack-number – Enables checking of acknowledgement number in RST packets which aborts a TCP flow in SYN (sent) state
  - validate-rst-seq-number – Enables checking of sequence number in RST packets which aborts an established TCP flow
- 

### Example

```
RFController(config-fw-policy-default)#ip dos tcp-max-incomplete high 8
RFController(config-fw-policy-default)#
```

```
RFController(config-fw-policy-default)# ip dos land log-only log-level
warnings
RFController(config-fw-policy-default)#
```

```
RFController(config-fw-policy-test)#ip tcp adjust-mss 475
RFController(config-fw-policy-test)#
```

```
RFController(config-fw-policy-test)#ip tcp recreate-flow-on-out-of-state-syn
RFController(config-fw-policy-test)#
```

```
RFController(config-fw-policy-test)#ip tcp validate-rst-seq-number
RFController(config-fw-policy-test)#
```



## ip-mac

### *firewall-policy*

Defines an action based on the IP MAC table

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ip-mac [conflict|routing]
ip-mac conflict [drop-only|log-and-drop|log-only]
ip-mac conflict [log-and-drop|log-only] log-level [<0-7>|
alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
ip-mac routing conflict [drop-only|log-and-drop|log-only]
ip-mac routing conflict [log-and-drop|log-only] log-level [<0-7>|
alerts|critical|debugging|emergencies|errors|informational|
notifications|warnings]
```

### Parameters

---

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [conflict routing] | <ul style="list-style-type: none"> <li>• conflict – Enables IP Address v. MAC Address conflict detection</li> <li>• routing – Defines action based on routing table</li> </ul> <p>The following are common for the above:</p> <ul style="list-style-type: none"> <li>• drop-only – Drops the packets</li> <li>• log-and-drop – Logs and drop the packets</li> <li>• log-only – Logs the packets only <ul style="list-style-type: none"> <li>• log-level – Configures the log level for DoS Checks <ul style="list-style-type: none"> <li>• &lt;0-7&gt; – Logging severity level</li> <li>• alerts – Immediate action needed (severity=1)</li> <li>• critical – Critical conditions (severity=2)</li> <li>• debugging – Debugging messages (severity=7)</li> <li>• emergencies – System is unusable (severity=0)</li> <li>• errors – Error conditions (severity=3)</li> <li>• informational – Informational messages (severity=6)</li> <li>• notifications – Normal but significant conditions (severity=5)</li> <li>• warnings – Warning conditions (severity=4)</li> </ul> </li> </ul> </li> </ul> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-fw-policy-default)#ip-mac conflict-detection log
RFController(config-fw-policy-default)#
```

## logging

### *firewall-policy*

Enables firewall enhanced logging

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
logging [icmp-packet-drop|malformed-packet-drop|verbose]
logging [icmp-packet-drop|malformed-packet-drop] [all|rate-limited]
```

### Parameters

[icmp-packet-drop|  
rawip-packet-drop]  
[all|rate-limited]

- icmp-packet-drop – Logs dropped ICMP packets failing sanity checks
- malformed-packet-drop – Logs dropped IP packets failing sanity checks

The following parameters are common for the above:

- all – Logs all message instances
- rate-limited – Enables rate-limiting. The granularity of rate-limiting is 20 seconds
- verbose – Enables verbose logging (applicable to selected platforms only)

### Example

```
RFController(config-fw-policy-default)#logging rawip-packet-drop all
RFController(config-fw-policy-default)#
```

```
RFController(config-fw-policy-test)#logging malformed-packet-drop
rate-limited
RFController(config-fw-policy-test)#
```

```
RFController(config-fw-policy-test)#logging verbose
RFController(config-fw-policy-test)#
```

## no

### *firewall-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [alg|clamp|dhcp-offer-convert|dns-snooping|firewall|flow|ip|
ip-mac|logging|proxy-arp|stateful-packet-inspection-l2 |storm-control|tcp|
virtual-defragmentation]
```

### Parameters

|                               |                                                                  |
|-------------------------------|------------------------------------------------------------------|
| alg                           | Disables alg                                                     |
| clamp                         | Deletes a clamp value                                            |
| dhcp-offer-convert            | Disables conversion broadcast DHCP offers to unicast             |
| dns-snoop                     | Disables DNS snooping                                            |
| firewall                      | Unconfigures the wireless firewall                               |
| flow                          | Defines a session flow timeout                                   |
| ip                            | Configures a selected <i>Internet Protocol</i> (IP) component    |
| ip-mac                        | Defines an action based on the IP-MAC table                      |
| logging                       | Disables firewall enhanced logging                               |
| proxy-arp                     | Disables generation of ARP responses on behalf of another device |
| stateful-packet-inspection-l2 | Disables stateful packet inspection in a layer2 firewall         |
| storm-control                 | Defines storm-control logging configuration                      |
| tcp                           | Disables the TCP protocol                                        |
| virtual-defragmentation       | Disables virtual defragmentation                                 |

### Example

```
RFController(config-fw-policy-default)#no storm-control arp log
RFController(config-fw-policy-default)#s

RFController(config-fw-policy-default)#no dhcp-offer-convert
RFController(config-fw-policy-default)#
```

## proxy-arp

### *firewall-policy*

Enables the generation of ARP responses on behalf of another device

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
proxy-arp
```

### **Parameters**

None

### **Example**

```
RFController(config-fw-policy-default)#proxy-arp  
RFController(config-fw-policy-default)#
```

## stateful-packet-inspection-12

### *firewall-policy*

Enables a stateful packet inspection at the layer2 firewall

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
stateful-packet-inspection-12
```

### **Parameters**

None

### **Example**

```
RFController(config-fw-policy-test)#stateful-packet-inspection-12  
RFController(config-fw-policy-test)#
```

## storm-control

### *firewall-policy*

Storm control limits the amount of multicast, unicast and broadcast frames accepted and forwarded by the device. Messages are logged based on their severity level.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
storm-control [arp|broadcast|multicast|unicast] [level|log]
storm-control [arp|bcast|mcast|ucast] level <1-1000000> [fe|ge|
port-channel|up1|wlan]
storm-control [arp|bcast|mcast|ucast] level <1-1000000> [fe <1-4>|ge <1-8>|
port-channel <1-8>|up1|wlan <WLAN>]
storm-control [arp|bcast|mcast|ucast] log [<0-7>|alert|critical|
debugging|emergencies|errors|informational|none|notifications
|warnings]
```

**Parameters**

[arp|bcast|mcast|ucast]{log}  
 [<0-7>|alert|critical  
 |debugging|  
 emergencies|errors|  
 informational|  
 none|notifications  
 |warnings]

- arp – The traffic type is ARP
- bcast – The traffic type is broadcast
- mcast – The traffic type is multicast
- ucast – The traffic type is unicast

For all the above, the following level and log options can be set

- level <1-1000000> [ge <1-8>|port-channel <1-8>|  
 up1|wlan <WLAN>] – Performs packet rate limiting
  - <1-1000000> – Specify the allowed rate in packets/sec from  
 <1-1000000>
  - ge <1-8> – Select a physical port to apply from 1-8
  - port-channel <1-8> – Select a port-channel from  
 1-8
  - up1 – Applies on the Uplink interface
  - wlan <WLAN> – Select a WLAN to apply. The existing WLAN must  
 be specified
- log – Enables logging
  - <0-8> – Select one numerical log level. All messages with and  
 below this severity are logged
  - emergencies – System is unusable (level 0)
  - alerts – Immediate action needed (level 1)
  - critical – Critical conditions (level 2)
  - errors – Error conditions (level 3)
  - warnings – Warning conditions (level 4)
  - notifications – Normal but significant conditions exist  
 (level 5)
  - informational – Informational messages (level 6)
  - debugging – Debugging messages (level 7)

**Example**

```
RFController(config-fw-policy-default)# storm-control unicast level 2 ge 2
RFController(config-fw-policy-default)#
```

```
RFController(config-fw-policy-default)#storm-control bcast log notifications
RFController(config-fw-policy-default)#
```

## virtual-defragmentation

### *firewall-policy*

Enables the virtual defragmentation for IPv4 packets

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
virtual-defragmentation {maximum-defragmentation-per-host <1-16384>|
maximum-fragments-per-datagram <2-8129>|minimum-first-fragment-length
<8-1500>}
```

### Parameters

|                                            |                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------|
| maximum-defragmentation-per-host <1-16384> | Defines the maximum active IPv4 defragmentations per host. Sets a value between 1 and 16384      |
| maximum-fragments-per-datagram <2-8129>    | Defines the maximum IPv4 fragments per datagram. Sets a value between 2 and 8129                 |
| minimum-first-fragment-length <8-1500>     | Defines the minimum length required for the first IPv4 fragment. Sets a value between 8 and 1500 |

### Example

```
RFController(config-fw-policy-test)#virtual-defragmentation
maximum-fragments-per-datagram 10
RFController(config-fw-policy-test)#

RFController(config-fw-policy-test)#virtual-defragmentation
minimum-first-fragment-length 100
RFController(config-fw-policy-test)#
```



# igmp-snoop-policy

## In this chapter

- [igmp-snoop-policy](#) ..... 703

This chapter summarizes the igmp-snoop-policy commands within the CLI structure.

Use the (config) instance to configure igmp-snoop-policy related configuration commands. To navigate to the config-igmp-snoop-policy instance, use the following commands:

```

RFController(config)#igmp-snoop-policy <policy-name>
RFController(config)#igmp-snoop-policy test

RFController(config-igmp-snoop-policy-test)#?
  igmp-snooping      Enable IGMP snooping
  no                  Negate a command or set its defaults
  querier            Configure IGMP querier
  robustness-variable Configure IGMP Robustness Variable
  unknown-multicast-fwd Forward Unknown Multicast Packet

  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

RFController(config-igmp-snoop-policy-test)#

```

## igmp-snoop-policy

Table 35 Summarizes igmp-snoop-policy commands

**TABLE 35** igmp-snoop-policy commands

| Command                               | Description                                 | Reference                |
|---------------------------------------|---------------------------------------------|--------------------------|
| <a href="#">igmp-snooping</a>         | Enables IGMP snooping                       | <a href="#">page 704</a> |
| <a href="#">querier</a>               | Configures IGMP querier                     | <a href="#">page 705</a> |
| <a href="#">robustness-variable</a>   | Configures IGMP Robustness variable         | <a href="#">page 706</a> |
| <a href="#">unknown-multicast-fwd</a> | Forwards unknown multicast packets          | <a href="#">page 707</a> |
| <a href="#">no</a>                    | Negates a command or sets its default value | <a href="#">page 708</a> |

## igmp-snooping

*igmp-snoop-policy*

Enables IGMP snooping

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
igmp-snooping
```

### Parameters

None

### Example

```
RFController(config-igmp-snoop-policy-test)#igmp-snooping  
RFController(config-igmp-snoop-policy-test)#
```

## querier

### *igmp-snoop-policy*

Configures the IGMP querier

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
querier query-interval <1-18000>
```

### Parameters

- 
- |                          |                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------|
| query-interval <1-18000> | • querier query-interval <1-18000> – Configures the IGMP querier value from the selected interval |
|                          | • <1-18000> – Select an interval between 1 and 18000                                              |
- 

### Example

```
RFController(config-igmp-snoop-policy-test)#querier query-interval 10
RFController(config-igmp-snoop-policy-test)#
```

## robustness-variable

### *igmp-snoop-policy*

Configures an IGMP robustness variable

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
robustness-variable <1-7>
```

### Parameters

---

|       |                                                             |
|-------|-------------------------------------------------------------|
| <1-7> | Select a value between 1 and 7 to configure IGMP robustness |
|-------|-------------------------------------------------------------|

---

### Example

```
RFController(config-igmp-snoop-policy-test)#robustness-variable 1
RFController(config-igmp-snoop-policy-test)#
```

## unknown-multicast-fwd

### *igmp-snoop-policy*

Forwards unknown multicast packets

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
unknown-multicast-fwd
```

### **Parameters**

None

### **Example**

```
RFController(config-igmp-snoop-policy-test)#unknown-multicast-fwd  
RFController(config-igmp-snoop-policy-test)#
```

**no***igmp-snoop-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [igmp-snooping | querier | robustness-variable | unknown-multicast-fwd]
```

**Parameters**


---

|                                                                                 |                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no[igmp-snooping   querier<br>  robustness-variable  <br>unknown-multicast-fwd] | <ul style="list-style-type: none"> <li>• igmp-snooping – Disables IGMP snooping</li> <li>• querier – Unconfigures the IGMP querier</li> <li>• robustness-variable – Reverts to the default IGMP robustness variable value</li> <li>• unknown-multicast-fwd – Does not forward unknown multicast packets</li> </ul> |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-igmp-snoop-policy-test)#no igmp-snooping
RFController(config-igmp-snoop-policy-test)#
```

**NOTE**

write, clrscr, do, exit, help, commit, revert, show, and service are common commands. For more information, see [Chapter 6, Common Commands](#).

---

# mint-policy

---

## In this chapter

- [mint-policy](#) ..... 710

This chapter summarizes mint-policy commands within the CLI 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 mint-policy instance, use the following commands:

```

RFController(config)#mint-policy global-default
RFController(config-mint-policy-global-default)#
RFController(config-mint-policy-global-default)#?
Mint Policy Mode commands:
  level                Mint routing level
  mtu                  Configure the global Mint MTU
  no                   Negate a command or set its defaults
  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

```

## mint-policy

[Table 36](#) Summarizes mint-policy commands

**TABLE 36** mint-policy commands

| <b>Command</b> | <b>Description</b>                              | <b>Reference</b>         |
|----------------|-------------------------------------------------|--------------------------|
| <i>level</i>   | Configures the MiNT routing level               | <a href="#">page 711</a> |
| <i>mtu</i>     | Configures the global MiNT MTU                  | <a href="#">page 712</a> |
| <i>no</i>      | Negates a command or sets its default value     | <a href="#">page 717</a> |
| <i>udp</i>     | Configures MiNT UDP/IP encapsulation parameters | <a href="#">page 716</a> |



## level

### *mint-policy*

Configures the MiNT routing level

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
level 2 area-id <1-4294967295>
```

### Parameters

---

|                          |                                                                                                                                                        |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 area-id <1-4294967295> | Configures level2 inter-site value                                                                                                                     |
|                          | <ul style="list-style-type: none"><li>• area-id &lt;1-4294967295&gt; – Configures routing area identifier value between &lt;1-4294967295&gt;</li></ul> |

---

### Example

```
RFController(config-mint-policy-global-default)#level 2 area-id 2
RFController(config-mint-policy-global-default)#

RFController(config-mint-policy-global-default)#show context
mint-policy global-default
  level 2 area-id 2
RFController(config-mint-policy-global-default)#
```

## mtu

### *mint-policy*

Configures the global MiNT MTU

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
mtu <900-1500>
```

### Parameters

---

|            |                                                                                           |
|------------|-------------------------------------------------------------------------------------------|
| <900-1500> | Specifies the maximum packet size. Will be rounded down to nearest (4 + a multiple of 8). |
|------------|-------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-mint-policy-global-default)#mtu 1000  
RFController(config-mint-policy-global-default)#
```

## re-join timeout

### *mint-policy*

Specifies the timeout after which the device attempts to join a new security domain

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
re-join timeout <30-4294967295>
```

### Parameters

---

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| <30-4294967295> | When unable to adopt, a device attempts to join a new security domain. Specify the timeout in seconds between 30 and 4294967295. |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-mint-policy-global-default)#rejoin-timeout 35  
RFController(config-mint-policy-global-default)#
```

## security-level

### *mint-policy*

Configures the MiNT security level used by all devices

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
security-level [control|control-and-data|none]
```

### Parameters

---

|                        |                                                                            |
|------------------------|----------------------------------------------------------------------------|
| [control               | • control – Configures MiNT security for control packets                   |
| control-and-data none] | • control-and-data – Configures MiNT security for control and data packets |
|                        | • none – No MiNT security                                                  |

---

### Example

```
RFController(config-mint-policy-global-default)#security-level
control-and-data
RFController(config-mint-policy-global-default)#
```

## sign-unknown-device

*mint-policy*

Accepts, sign and certificate signing requests from unknown devices automatically

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
sign-unknown-device
```

### Parameters

None

### Example

```
RFController(config-mint-policy-global-default)#sign-unknown-device  
RFController(config-mint-policy-global-default)#
```

## udp

### *mint-policy*

Configures MiNT UDP/IP encapsulation parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
udp port <2-65534>
```

### Parameters

---

|                |                                                                                              |
|----------------|----------------------------------------------------------------------------------------------|
| port <2-65534> | Configures the default UDP port used for MiNT control packet encapsulation between <2-65534> |
|----------------|----------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-mint-policy-global-default)#udp port 1024  
RFController(config-mint-policy-global-default)#
```

## no

### *mint-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [level|mtu|udp|rejoin-timeout|security-level|sign-unknown-device]
```

### Parameters

---

|                      |                                                                  |               |
|----------------------|------------------------------------------------------------------|---------------|
| no [level mtu udp    | • rejoin-timeout – Resets the rejoin timeout to its default      |               |
| rejoin-timeout       | • security-level – Resets the MiNT security level to its default |               |
| security-level       | • sign-unknown-device – Disables automatic certificate signing   |               |
| sign-unknown-device] | • level – Resets MiNT routing level                              |               |
|                      | • mtu – Uses default global MiNT MTU                             |               |
|                      | • udp – Resets MiNT UDP/IP encapsulation to default              | configuration |

---

### Example

```
RFController(config-mint-policy-global-default)#no sign-unknown-device
RFController(config-mint-policy-global-default)#
```

### NOTE

The commands `clear`, `commit`, `exit`, `end`, `help`, `write`, `revert`, `service` and `show` are common commands. For more information, see [Chapter 6, Common Commands](#).

---





# management-policy

---

## In this chapter

- [management-policy..... 720](#)

This chapter summarizes management-policy commands within the CLI structure.

Use the (config) instance to configure management-policy related configuration commands. To navigate to the management-policy instance, use the following commands:

```
RFController(config)#management-policy <policy-name>
RFController(config)#management-policy default
```

To commit a management-policy, at least one admin user account must always be present in the management-policy:

```
RFController(config-management-policy-default)#user superuser password 1
admin123
RFController(config-management-policy-default)#commit
RFController(config-management-policy-default)#
RFController(config-management-policy-default)#?
aaa-login      Set authentication for logins
banner        Define a login banner  exec-timeout  Configure timeout in
seconds
ftp           Enable FTP server
http         Hyper Text Terminal Protocol (HTTP)
https        Secure HTTP
no           Negate a command or set its defaults
restrict-access  Restrict management access to the device
snmp-server  SNMP
ssh          Enable ssh
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
RFController(config-management-policy-default)#
```

## management-policy

Table 37 Summarizes management-policy commands

**TABLE 37** management-policy commands

| Command                         | Description                                              | Reference                |
|---------------------------------|----------------------------------------------------------|--------------------------|
| <a href="#">aaa-login</a>       | Sets authentication for logins                           | <a href="#">page 721</a> |
| <a href="#">banner</a>          | Defines a login banner name                              | <a href="#">page 723</a> |
| <a href="#">ftp</a>             | Enables a FTP server                                     | <a href="#">page 724</a> |
| <a href="#">http</a>            | Enables a HTTP server                                    | <a href="#">page 726</a> |
| <a href="#">https</a>           | Enables a secure HTTPs server                            | <a href="#">page 727</a> |
| <a href="#">no</a>              | Negates a command or sets its default value              | <a href="#">page 728</a> |
| <a href="#">restrict-access</a> | Restricts management access to a set of hosts or subnets | <a href="#">page 729</a> |
| <a href="#">snmp-server</a>     | Sets the SNMP-server configuration                       | <a href="#">page 730</a> |
| <a href="#">ssh</a>             | Enables SSB                                              | <a href="#">page 733</a> |
| <a href="#">telnet</a>          | Enables Telnet                                           | <a href="#">page 734</a> |
| <a href="#">user</a>            | Creates a new user account                               | <a href="#">page 735</a> |

## aaa-login

### *management-policy*

Configures the current authentication, authorization and accounting (aaa) login settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
aaa-login [local|radius]
aaa-login radius [external|fallback|server]
aaa-login radius server host <A.B.C.D> secret [0|2] <WORD> {attempts
<1-10>|time-out <1-60>|udp-port <0-65536>}
```

### Parameters

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| local                             | Sets local authentication                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| radius [external fallback server] | <p>Configures an external RADIUS server</p> <ul style="list-style-type: none"> <li>• external – Requires external RADIUS authentication</li> <li>• fallback – Attempts external RADIUS authentication, uses local authentication when failed</li> <li>• server host &lt;A.B.C.D&gt; secret [0 2] &lt;WORD&gt; {attempts &lt;1-10&gt;  time-out &lt;1-60&gt;   udp-port &lt;0-65536&gt;} – Defines an external RADIUS server <ul style="list-style-type: none"> <li>• host – Sets the IP address of RADIUS server to configure <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Specify the IP address of RADIUS server to configure <ul style="list-style-type: none"> <li>• secret [0 2] &lt;WORD&gt; – Enter a clear text secret</li> <li>• 0 – Password is encrypted with secret</li> <li>• 2 – Password is UNENCRYPTED</li> <li>• &lt;WORD&gt; – Enter text of shared secret, up to 127 characters</li> <li>• attempts &lt;1-10&gt; – Specifies the number of attempts to connect to RADIUS server</li> <li>• timeout &lt;1-60&gt; – Specify the timeout value between 1and 60 seconds for the server's response</li> <li>• udp-port &lt;0-65536&gt; – Specify the UDP port number for the RADIUS server. The default port is 1812</li> </ul> </li> </ul> </li> </ul> </li> </ul> |

### Usage Guidelines

Use an AAA login to determine whether management user authentication must be performed against a local user database or an external RADIUS server

## 18 management-policy

### Example

```
RFController(config-management-policy-default)#aaa-login radius radius-server
host 172.16.10.9 udp-port 3
RFController(config-management-policy-default)#

RFController(config-management-policy-default)#aaa-login local
RFController(config-management-policy-default)#
```

## banner

### *management-policy*

Defines the login banner message

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
banner motd <LINE>
```

### Parameters

---

|             |                                    |
|-------------|------------------------------------|
| motd <LINE> | Sets the message of the day banner |
|-------------|------------------------------------|

---

### Example

```
RFController(config-management-policy-default)#banner motd GoodDay
RFController(config-management-policy-default)#
```

## ftp

### *management-policy*

Configures FTP server parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ftp {password [1 <WORD>|<WORD>]|rootdir <DIR>|username}
ftp username <WORD> password [1 <WORD> rootdir <DIR>|<WORD> rootdir <DIR>]
```

### Parameters

|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| password [1 <WORD> <WORD>]                                             | Configures ftp password <ul style="list-style-type: none"> <li>• 1 &lt;WORD&gt; – Enter the encrypted password (Eg: if copy-pasting from another device)</li> <li>• &lt; WORD&gt; – Enter the password</li> </ul>                                                                                                                                                                                                                                                                                                                                                                   |
| rootdir <DIR>                                                          | Configures a FTP root directory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| username <WORD> password [1 <WORD> rootdir <DIR> <WORD> rootdir <DIR>] | Defines a FTP username <ul style="list-style-type: none"> <li>• password – Configures the FTP password <ul style="list-style-type: none"> <li>• 1 &lt;WORD&gt; rootdir &lt;DIR&gt; – Enter the encrypted password (Eg: if copy-pasting from another device) <ul style="list-style-type: none"> <li>• rootdir &lt;DIR&gt; – Sets the ROOT directory location of the FTP server <ul style="list-style-type: none"> <li>• &lt;DIR&gt; – The root directory for the FTP server</li> </ul> </li> </ul> </li> <li>• &lt;WORD&gt; – Enter the password to configure</li> </ul> </li> </ul> |

### Usage Guidelines

The string size of encrypted password (option 1, Password is encrypted with SHA1 algorithm) must be exactly 40 characters.

**Example**

```
RFController(config-management-policy-test)#ftp password word
RFController(config-management-policy-test)#

RFController(config-management-policy-test)#ftp password 1 root
RFController(config-management-policy-test)#

RFController(config-management-policy-test)#ftp rootdir dir
RFController(config-management-policy-test)#

RFController(config-management-policy-test)#ftp username superuser password 1
word rootdir dir
RFController(config-management-policy-test)#
RFController(config-management-policy-test)#show context
management-policy test
  http server
  ftp username root password 1 word rootdir dir
  no ssh
  user superuser password 1
4e03aaf1065294ba86d19da984347e38dfbaa9955335dc354748cb4f9a16e0a9
RFController(config-management-policy-test)#
```

## http

### *management-policy*

Defines HTTP server settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
http <server>
```

### Parameters

---

|        |                         |
|--------|-------------------------|
| server | Enables the HTTP server |
|--------|-------------------------|

---

### Example

```
RFController(config-management-policy-test)#http server  
RFController(config-management-policy-test)#
```



## https

### *management-policy*

Configures secure HTTPs server parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
https server
```

### Parameters

---

|        |                          |
|--------|--------------------------|
| server | Enables the HTTPS server |
|--------|--------------------------|

---

### Example

```
RFController(config-management-policy-test)#https server trustpoint testtrust  
RFController(config-management-policy-test)#
```

**no***management-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [banner|exec-timeout|ftp|http|https|secure-management|
snmp-server|ssh|telnet|user]
```

**Parameters**


---

|                      |                                                         |
|----------------------|---------------------------------------------------------|
| [banner exec-timeout | • banner – Defines a login banner                       |
| ftp http https       | • exec-timeout – Disables the session timeout           |
| secure-management    | • ftp – Enables a FTP server                            |
| snmp-server          | • http – Enables the hypertext terminal protocol (HTTP) |
| ssh telnet user]     | • https – Enables secure HTTP                           |
|                      | • secure-management – Disables secure management        |
|                      | • snmp-server – Disables SNMP                           |
|                      | • ssh – Disables SSH                                    |
|                      | • telnet – Disables Telnet                              |
|                      | • user – Removes user account                           |

---

**Example**

```
RFController(config-management-policy-test)#no ssh port
RFController(config-management-policy-test)#
```

```
RFController(config-management-policy-test)#no secure-management
RFController(config-management-policy-test)#
```

## restrict-access

### management-policy

Restricts management access to a set of hosts or subnets

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
restrict-access [host|ip-access-list|subnet]
restrict-access host <A.B.C.D> {<A.B.C.D>/log [all|denied-only]/subnet
<A.B.C.D/M> {<A.B.C.D>/M/log [all|denied-only]}}
restrict-access ip-access-list <IP-ACCESS-LIST>
restrict-access subnet <A.B.C.D/M> {<A.B.C.D>/M/log [all|denied-only]/host
<A.B.C.D> {<A.B.C.D>/log [all|denied-only]}}
```

### Parameters

- 
- |                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [host ip-access-list subnet] | <ul style="list-style-type: none"> <li>• host &lt;A.B.C.D&gt; {&lt;A.B.C.D&gt;/log [all denied-only]/subnet &lt;A.B.C.D/M&gt; {&lt;A.B.C.D&gt;/M/log [all denied-only]}} – Restricts management access to specific hosts</li> <li>• ip-access-list &lt;IP-ACCESS-LIST&gt; – Uses an IP access list to filter requests for management access <ul style="list-style-type: none"> <li>• &lt;IP-ACCESS-LIST&gt; – Specify the IP access list to be used</li> </ul> </li> <li>• subnet&lt;A.B.C.D/M&gt; {&lt;A.B.C.D&gt;/M/log [all denied-only]/host &lt;A.B.C.D&gt; {&lt;A.B.C.D&gt;/log [all denied-only]}} – Restricts management access to specific subnets <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt;/M – Specify a subnet IP to restrict management access</li> </ul> </li> </ul> |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The following parameters are common for all the above:

- log – Configures logging policy for management access
  - all – Logs all the requests for management access (includes denied and permitted)
  - denied-only – Logs denied requests for management access
- 

### Example

```
RFController(config-management-policy-default)#restrict-access host
172.16.10.2 log all
RFController(config-management-policy-default)#
```

```
RFController(config-management-policy-default)#restrict-access subnet
172.16.10.20/24 host 1.2.3.4 log all
RFController(config-management-policy-default)#
```

```
RFController(config-management-policy-default)#restrict-access host 1.2.3.4
log denied-only
RFController(config-management-policy-default)#
```

## snmp-server

### management-policy

Configures SNMP engine parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
snmp-server [community|enable|host|manager|user]
snmp-server enable traps
snmp-server community <WORD> [ro|tw]
snmp-server host <A.B.C.D> [v2c|v3] {<1-65535>}
snmp-server manager [all|v2|v3]
snmp-server user [snmpmanager|snmpoperator|snmptrap] v3 [auth md5|encrypted
[auth md5|des auth md5][0|2|<WORD>]
```

### Parameters

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| community <WORD> [ro tw]            | Sets the community string and access privileges. <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Sets the community string <ul style="list-style-type: none"> <li>• ro – Assigns read-only access to this community string</li> <li>• rw – Assigns read-write access to this community string</li> </ul> </li> </ul>                                                                           |
| enable traps                        | Enables SNMP traps                                                                                                                                                                                                                                                                                                                                                                                     |
| host <A.B.C.D> [v2c v3] {<1-65535>} | SNMP server host <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; – Sets the SNMP server host IP address <ul style="list-style-type: none"> <li>• v2c – Use SNMP version 2c</li> <li>• v3 – Use SNMP version 3 <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; – Select a value between 1 and 65535 to configure the port. The default port is 162</li> </ul> </li> </ul> </li> </ul> |

---

|                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>manager [all   v2   v3]</code>                                                                                                                            | <p>Enables SNMP manager</p> <ul style="list-style-type: none"> <li>• all – Enables SNMP version v2 and v3</li> <li>• v2 – Enables SNMP version v2</li> <li>• v3 – Enable SNMP version v3</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>snmp-server user<br/>[snmpmanager   snmpoperator   sn<br/>mptrap] v3 [auth md5   encrypted<br/>[auth md5   des auth<br/>md5][0   2   &lt;WORD&gt;]</code> | <p>Defines a user who can access the SNMP engine</p> <ul style="list-style-type: none"> <li>• snmpmanager – Sets the user as a manager</li> <li>• snmpoperator – Sets the user as an operator</li> <li>• snmptrap – Sets the user as a SNMP trap user</li> </ul> <p>The following parameters are common for all the above types of users:</p> <ul style="list-style-type: none"> <li>• v3 [auth md5   encrypted] – Use the SNMPv3 as the security model <ul style="list-style-type: none"> <li>• auth md5 – Authentication protocol <ul style="list-style-type: none"> <li>• md5 – Uses the HMAC-MD5 algorithm for authentication</li> </ul> </li> <li>• encrypted [auth   des] – Encrypted protocol</li> <li>• auth md5 – Sets authentication parameters for the user <ul style="list-style-type: none"> <li>• md5 [0   2   &lt;WORD&gt;] – Uses the HMAC-MD5 algorithm for authentication <ul style="list-style-type: none"> <li>• 0 – Enter a clear text password</li> <li>• 2 – Enter an encrypted password</li> <li>• &lt;WORD&gt; – Specify a password for authentication and privacy protocols</li> </ul> </li> </ul> </li> <li>• des – Uses CBC-DES for privacy</li> </ul> </li> </ul> |

---

**Example**

```

RFController(config-management-policy-test)#snmp-server community snmp1 ro
RFController(config-management-policy-test)#

RFController(config-management-policy-test)#snmp-server host 172.16.10.23 v3
162
RFController(config-management-policy-test)#commit
RFController(config-management-policy-test)#

RFController(config-management-policy-test)#snmp-server user snmpmanager v3
auth md5 admin123
RFController(config-management-policy-test)#
RFController(config-management-policy-test)#show context
management-policy test
  http server
  https server trustpoint testtrust
  ftp username root password 1 word rootdir dir
  no ssh
  user superuser password 1
4e03aaf1065294ba86d19da984347e38dfbaa9955335dc354748cb4f9a16e0a9
snmp-server community snmp1 ro
snmp-server enable traps
snmp-server host 172.16.10.23 v3 162
snmp-server host 172.16.10.3 v3 162
snmp-server host 172.16.10.23 v2c 4
RFController(config-management-policy-test)#

```

## ssh

### *management-policy*

Configures SSH parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ssh {port} <1-65535>
```

### Parameters

---

|                |                                                                                           |
|----------------|-------------------------------------------------------------------------------------------|
| port <1-65535> | Select a value between 1 and 165535 to configure a SSH port. The default port value is 22 |
|----------------|-------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-management-policy-test)#ssh port 162 ?  
RFController(config-management-policy-test)#
```

## telnet

### *management-policy*

Enables Telnet settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
telnet {port} <1-65535>
```

### Parameters

---

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| port <1-65535> | Select a Telnet port value between 1 and 165535. The default port is 23. |
|----------------|--------------------------------------------------------------------------|

---

### Example

```
RFController(config-management-policy-test)#telnet port 23  
RFController(config-management-policy-test)#
```



## user

### *management-policy*

Creates a new user account

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
user <WORD> password [0|1|<WORD>]
user <WORD> password [0|1|<WORD>] role [helpdesk|monitor|
network-admin|security-admin|superuser|system-admin|web-user-admin] access
[all|console|ssh|telnet]
user <WORD> password [0|1|<WORD>] role [helpdesk|monitor|
network-admin|security-admin|superuser|system-admin|web-user-admin] access
{all|console|ssh|telnet}
```

### Parameters

- 
- |                 |                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <WORD> password | <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify a user account name to create an user account</li> <li>• password – Specify a user password <ul style="list-style-type: none"> <li>• 0 – Enter the clear text password</li> <li>• 1 – Enter an encrypted password</li> <li>• &lt;WORD&gt; – Enter the password to configure</li> </ul> </li> </ul> |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The following parameters are common for both encrypted password and generic password

- role [helpdesk | monitor | network-admin | security-admin | superuser | system-admin | web-user-admin] access [all | console | ssh | telnet] – Configures a role for the new user, assign a role from the list:
    - helpdesk – Helpdesk
    - monitor – Monitor
    - network-admin – Network administrator
    - security-admin – Security administrator
    - superuser – Superuser
    - system-admin – System administrator
    - web-user-admin – Web user administrator
    - access – Configures user access
    - all – Allow access to all the modes
    - console – Allows console access
    - ssh – Allows SSH access
    - telnet – Allows Telnet access
-

## Example

```
RFController(config-management-policy-test)#user testuser password brocade123
RFController(config-management-policy-test)#commit
RFController(config-management-policy-default)#user george password 1 admin12
role security-admin access console ssh telnet web
RFController(config-management-policy-default)#
```

---

## NOTE

The commands `clrsr`, `commit`, `do`, `exit`, `help`, `write`, `revert`, `service` and `show` are common commands. Refer to [Chapter 6, Common Commands](#) for more information.

---

## radius-policy

## In this chapter

- radius-group ..... 738
- radius-server-policy ..... 744
- radius-user-pool-policy ..... 756

This chapter summarizes RADIUS-Group, RADIUS-Server, and RADIUS-User-Policy commands in detail.

Use the (config) instance to configure RADIUS-Group related configuration commands. This command creates a group within the existing RADIUS group. To navigate to the radius-group instance, use the following commands:

```

RFController(config)#radius-group <group-name>
RFController(config)#radius-group test
RFController(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

RFController(config-radius-group-test)#

```

## radius-group

Sets RADIUS user group parameters

[Table 38](#) Summarizes radius-group commands

**TABLE 38** radius-group commands

| Command                    | Description                                                                       | Reference                |
|----------------------------|-----------------------------------------------------------------------------------|--------------------------|
| <a href="#">guest</a>      | Enables guest access for the newly created group                                  | <a href="#">page 739</a> |
| <a href="#">policy</a>     | Configures RADIUS group access policy parameters                                  | <a href="#">page 740</a> |
| <a href="#">rate-limit</a> | Sets the default rate limit per user in kbps, and applies it to all enabled WLANs | <a href="#">page 742</a> |
| <a href="#">no</a>         | Negates a command or sets its default values                                      | <a href="#">page 743</a> |

## guest

### *radius-group*

Manages a guest user linked with a hotspot. Create a guest-user and associate it with the guest group. The guest user and policies are used for hotspot authentication/authorization.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
guest
```

### **Parameters**

None

### **Example**

```
RFController(config-radius-group-test)#guestRFController(config-radius-group-test)#
```

## policy

### *radius-group*

Sets the authorization policies for a particular group day/time of access, WLANs etc.

---

#### NOTE

A user-based VLAN is effective only if dynamic VLAN authorization is enabled for the WLAN (as defined within the WLAN Configuration screen).

---

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### Syntax

```
policy [access|day|role|ssid|time|vlan <1-4094>]
policy access [all|console|ssh|telnet|web]
policy access [all|console|ssh|telnet|web] {all/console/ssh/telnet/web}
policy role [helpdesk|monitor|network-admin|security-admin|
super-user|system-admin|web-user-admin]
policy ssid <WORD>
policy day[all|fri|mo|sa|su|tu|we|th|weekdays]{all/fri/mo/sa/su/tu/
we/th/weekdays}
policy time start <HH:MM> end <HH:MM>
```

**Parameters**

|                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access<br>[all   console   ssh   telnet   web]                                                          | Sets management group access <ul style="list-style-type: none"> <li>• all – Allows all access</li> <li>• console – Allows console access</li> <li>• ssh – Allows SSH access</li> <li>• telnet – Allows Telnet access</li> <li>• web – Allows Web access</li> </ul>                                                                                                                                |
| day<br>[all   fri   mo   sa   su   th   tu   we   week days]                                            | Configures the access day for this group <ul style="list-style-type: none"> <li>• all – All days (from Sunday to Saturday)</li> <li>• fri – Friday</li> <li>• mo – Monday</li> <li>• sa – Saturday</li> <li>• su – Sunday</li> <li>• th – Thursday</li> <li>• tu – Tuesday</li> <li>• we – Wednesday</li> <li>• weekdays – Configures the policy access in weekdays (Monday to Friday)</li> </ul> |
| role [helpdesk   monitor   network-admin   security-admin   super-user   system-admin   web-user-admin] | Sets the management group role <ul style="list-style-type: none"> <li>• helpdesk – Helpdesk</li> <li>• monitor – Monitor</li> <li>• network-admin – Network administrator</li> <li>• security-admin – Security administrator</li> <li>• superuser – Superuser</li> <li>• system-admin – System administrator</li> <li>• web-user-admin – Web user administrator</li> </ul>                        |
| ssid <WORD>                                                                                             | Configures SSID for this group <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify a case-sensitive alphanumeric SSID, up to 32 characters</li> </ul>                                                                                                                                                                                                                                 |
| time start<HH:MM> end <HH:MM>                                                                           | Configures time of access for this group <ul style="list-style-type: none"> <li>• start &lt;HH:MM&gt; – Enter the start time in the format: HH:MM for ex., 13:30 means user can login only after 1:30 PM</li> <li>• end&lt;HH:MM&gt; – Enter the end time in the format: HH:MM for ex., 17:30 means that until 5:30 PM, the user is allowed to remain logged in</li> </ul>                        |
| vlan <1-4094>                                                                                           | Select a value between 1 and 4094 to configure a VLAN ID for this group                                                                                                                                                                                                                                                                                                                           |

**Example**

```

RFController(config-radius-group-test)#policy time start 13:30 end 17:30
RFController(config-radius-group-test)#

RFController(config-radius-group-test)#policy wlan wlan1
RFController(config-radius-group-test)#

RFController(config-radius-group-test)#show context
radius-group test
  guest-group
  policy vlan 2
  policy wlan wlan1
  policy time start 13:30 end 17:30
RFController(config-radius-group-test)#

```

## rate-limit

### *radius-group*

Sets the rate limit for the RADIUS server group

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
rate-limit [from-air|to-air] <100-1000000>
```

### Parameters

|                        |                                                                                                                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| to-air <100-1000000>   | Downlink direction from the network to wireless client <ul style="list-style-type: none"> <li>• &lt;100-1000000&gt; - Specifies the rate in the range of &lt;100-1000000&gt;</li> </ul> |
| from-air <100-1000000> | Uplink direction from wireless client to the network <ul style="list-style-type: none"> <li>• &lt;100-1000000&gt; - Specifies the rate in the range of &lt;100-1000000&gt;</li> </ul>   |

### Usage Guidelines

Use `[no] rate-limit [wired-to-wireless|wireless-to-wired]` to remove the rate limit applied to the group.

`[no] rate-limit [wireless-to-wired]` sets the rate limit back to unlimited

### Example

```
RFController(config-radius-group-test)##rate-limit to-air 101
RFController(config-radius-group-test)#
```



## no

### *radius-group*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [guest|policy|rate-limit]
```

### Parameters

---

|                          |                                                                                                                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| guest policy rate-limit] | <ul style="list-style-type: none"><li>• guest – Makes this group a non-guest group</li><li>• policy – Removes RADIUS group access policy configuration</li><li>• rate-limit – Removes rate-limit for the RADIUS group</li></ul> |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-radius-group-test)#no guest
RFController(config-radius-group-test)#
```

## radius-server-policy

Creates an onboard device RADIUS policy

Use the (config) instance to configure RADIUS-Server-Policy related configuration commands. To navigate to the RADIUS-Server-Policy instance, use the following commands:

```
RFController(config)#radius-server-policy <policy-name>
RFController(config)#radius-server-policy test
RFController(config-radius-server-policy-test)#
```

**Table 39** Summarizes radius-server-policy commands

**TABLE 39** radius-server-policy commands

| Commands                       | Description                                               | Reference                |
|--------------------------------|-----------------------------------------------------------|--------------------------|
| <i>authentication</i>          | Configures RADIUS authentication parameters               | <a href="#">page 745</a> |
| <i>crl-check</i>               | Enables certificate revocation list (CRL) check           | <a href="#">page 746</a> |
| <i>ldap-group-verification</i> | Enables LDAP group verification settings                  | <a href="#">page 747</a> |
| <i>ldap-server</i>             | Configures LDAP server parameters                         | <a href="#">page 748</a> |
| <i>local</i>                   | Configures a local RADIUS realm                           | <a href="#">page 750</a> |
| <i>nas</i>                     | Configures the key that must be sent to the RADIUS client | <a href="#">page 751</a> |
| <i>no</i>                      | Negates a command or sets its default value               | <a href="#">page 752</a> |
| <i>proxy</i>                   | Configures RADIUS proxy server settings                   | <a href="#">page 753</a> |
| <i>session-resumption</i>      | Enables session resumption                                | <a href="#">page 754</a> |
| <i>use</i>                     | Defines settings used with the RADIUS Server Policy       | <a href="#">page 755</a> |

## authentication

### *radius-server-policy*

Configures RADIUS authentication parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
authentication [data-source|eap-auth-type]
authentication data-source [ldap|local]
authentication eap-auth-type [all|peap-gtc|peap-mschapv2|tls|ttls-md5|
ttls-mschapv2|ttls-pap]
```

### Parameters

|                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| data-source [ldap local]                                                                  | <p>Enables the RADIUS data source for user authentication</p> <ul style="list-style-type: none"> <li>• ldap – Remote LDAP server</li> <li>• local – Local user database</li> </ul>                                                                                                                                                                                                                                                                                                                                                        |
| eap-auth-type<br>[all peap-gtc peap-mschapv2 <br>tls ttls-md5 <br>ttls-mschapv2 ttls-pap] | <p>Enables RADIUS EAP and default authentication type configuration</p> <ul style="list-style-type: none"> <li>• all – Enables both ttls and peap</li> <li>• peap-gtc – Eap type peap with default auth type gtc</li> <li>• peap-mschapv2 – EAP type peap with default auth type mschapv2</li> <li>• tls – EAP type tls</li> <li>• ttls-md5 – EAP type ttls with default auth type md5</li> <li>• ttls-mschapv2 – EAP type ttls with default auth type mschapv2</li> <li>• ttls-pap – EAP type ttls with default auth type pap</li> </ul> |

### Example

```
RFController(config-radius-server-policy-test)#authentication eap-auth-type
tls
RFController(config-radius-server-policy-test)#
```

## crl-check

*radius-server-policy*

Enables certificate revocation list (CRL) check

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
crl-check
```

### Parameters

None

### Example

```
RFController(config-radius-server-policy-test)#crl-check  
RFController(config-radius-server-policy-test)#
```

## ldap-group-verification

*radius-server-policy*

Enables LDAP group verification settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ldap-group-verification
```

### Parameters

None

### Example

```
RFController(config-radius-server-policy-test)#ldap-group-verification  
RFController(config-radius-server-policy-test)#
```

## ldap-server

*radius-server-policy*

Configures LDAP server parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ldap-server [dead-period <0-600>|primary|secondary]
ldap-server [primary|secondary] host <A.B.C.D> port <1-65535> login <WORD>
bind-dn <WORD> base-dn <WORD> passwd [0|2|<WORD>] passwd-attr <WORD>
group-attr <WORD> group-filter <WORD> group-membership <WORD> {net-timeout}
<1-10>
```

## Parameters

```
[primary|secondary] host
<A.B.C.D> port
<1-65535> login <WORD>
bind-dn <WORD> base-dn
<WORD> passwd 0 <WORD>
passwd-attr <WORD> group-attr
<WORD> group-filter <WORD>
group-membership <WORD>
{net-timeout} <1-10>
```

- primary – Configures the primary LDAP server configuration
  - secondary – Configures the secondary LDAP server configuration
- The following configuration parameters are common for both the primary and secondary LDAP servers:
- host – Configures LDAP server IP configuration
  - <A.B.C.D> – Specify the LDAP server IP address to configure
  - port <1-65535> – Select a value between 1 and 65535 to configure a port
  - login <WORD> – Specify a name to configure LDAP server name. The maximum login size is 127
  - maximum size is 127
  - bind-dn <WORD> – Specify a distinguished bind name. The maximum bind-distinguished name size is 127 characters
  - base-dn <WORD> – Specify a name to configure base distinguished name. The maximum size is 127 characters
  - passwd [<0>|2|<WORD>] – Specify a name to configure LDAP server password. 0 specifies UNENCRYPTED password. 2 specifies ENCRYPTED password. The LDAP server bind password size is 31
  - passwd-attr <WORD> – Specify a name to configure LDAP server password attribute. The maximum size is 63 characters
  - group-attr <WORD> – Specify a name to configure group attributes. The maximum size is 31 characters
  - group-filter <WORD> – Specify a name for the group-filter attribute. The maximum size is 255 characters
  - group-membership <WORD> – Specify a name for the group membership attribute. 63 is the maximum character size
  - {net-timeout} <1-10> – Select a value between 1 and 15 to configure network timeout value (number of seconds to wait for response of the server (network failures))

## Example

```
RFController(config-radius-server-policy-test)#ldap-server primary host
172.16.10.19 port 162 login brocade bind-dn bind-dn1 base-dn base-dn1 passwd 0
brocade passwd-attr brocade123 group-attr gropl group-filter gropfilter1
group-membership gropmember
ship1 net-timeout 2
```

```
RFController(config-radius-server-policy-test)#ldap-server secondary host
172.16.10.2 port 2 login word bind-dn word1 base-
dn word2 passwd 0 word4 passwd-attr word4 group-attr word5 group-filter word6
group-membership word8 net-timeout 3
RFController(config-radius-server-policy-test)#
```

```
RFController(config-radius-server-policy-test)#show context
radius-server-policy test
authentication data-source ldap
crl-check
ldap-server primary host 172.16.10.19 port 162 login brocade bind-dn bind-dn1
base-dn base-dn1 passwd 0 brocade passwd-attr brocade123 group-attr gropl
group-filter gropfilter1 group-membership gropmembersh1 net-timeout 2
RFController(config-radius-server-policy-test)#
```

## local

### *radius-server-policy*

Configures a local RADIUS realm

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
local realm <WORD>
```

### Parameters

---

|              |                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| realm <WORD> | Configures a local RADIUS realm <ul style="list-style-type: none"><li>• &lt;WORD&gt; – Specify a local RADIUS realm name. Use a string of up to 50 characters</li></ul> |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-radius-server-policy-test)#local realm realm1  
RFController(config-radius-server-policy-test)#
```



## nas

### *radius-server-policy*

Configures the key sent to a RADIUS client

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
nas <A.B.C.D/M> secret [0|2|<LINE>]
```

### Parameters

- 
- <A.B.C.D/M> secret [0|2|<LINE>] Sets the RADIUS client's IP address
- secret – Sets the RADIUS client's shared secret
    - 0 – Secret is specified UNENCRYPTED
    - 2 – Secret is specified ENCRYPTED
    - <LINE> – Defines the secret (client shared secret) up to 32 characters.
- 

### Example

```
RFController(config-radius-server-policy-test)#nas 172.16.10.10/24 key 0  
wirelesswell  
RFController(config-radius-server-policy-test)#
```

**no***radius-server-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [authentication|clr-check|ldap-group-verification|
    ldap-server|local|nas|proxy|session-resumption|use]
```

**Parameters**


---

|                           |                                                                       |
|---------------------------|-----------------------------------------------------------------------|
| [authentication clr-check | • authentication – Unconfigures RADIUS authentication                 |
| ldap-group-verification   | • cri-check – Unconfigures a CRL check                                |
| ldap-server local         | • ldap-group-verification – Disables LDAP group verification settings |
| nas proxy                 | • ldap-server – Unconfigures LDAP server parameters                   |
| session-resumption use]   | • local – Unconfigures RADIUS local realm value                       |
|                           | • nas – Unconfigures the RADIUS client                                |
|                           | • proxy – Unconfigures the RADIUS proxy server                        |
|                           | • session-resumption – Disables session resumption                    |

---

**Example**

```
RFController(config-radius-server-policy-test)#no use server-trustpoint
RFController(config-radius-server-policy-test)#

RFController(config-radius-server-policy-test)#no no local realm all
RFController(config-radius-server-policy-test)#
```

## proxy

### *radius-server-policy*

Configures a proxy RADIUS server based on the realm/suffix

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
proxy [realm|retry-count|retry-delay]
proxy realm <WORD> server <A.B.C.D> port <1024-65535> secret [0|2|<WORD>]
proxy retry-count <3-6>
proxy retry-delay <5-10>
```

### Parameters

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| realm <WORD> server <A.B.C.D><br>port<br><1024-65535> secret 0 <WORD> | <p>The realm name is a string of up to 50 characters</p> <ul style="list-style-type: none"> <li>• server &lt;A.B.C.D&gt; – Specify an IP address to configure proxy server</li> <li>• port &lt;1024-65535&gt; – Select a value between 1024 and 65535 to configure proxy server port</li> <li>• secret [0 2 &lt;WORD&gt;] – Sets the proxy server secret string           <ul style="list-style-type: none"> <li>• 0 – Password is specified UNENCRYPTED</li> <li>• 2 – Password is specified ENCRYPTED</li> <li>• &lt;WORD&gt; – Specify the proxy server shared secret value. Can be up to 31 characters</li> </ul> </li> </ul> |
| retry-count <3-6>                                                     | Select a value between 3 and 6 to configure the proxy server retry count                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| retry-delay <5-10>                                                    | Select a value between 5 and 10 seconds to configure the proxy server retry delay time                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### Usage Guidelines

Only 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 the controller transmits each RADIUS request before giving up. The timeout value defines the duration for which the controller waits for a reply to a RADIUS request before retransmitting the request.

### Example

```
RFController(config-radius-server-policy-test)#proxy realm test1 server
172.16.10.7 port 1025 secret 0 admin123
RFController(config-radius-server-policy-test)#

RFController(config-radius-server-policy-test)#proxy retry-count 4
RFController(config-radius-server-policy-test)#

RFController(config-radius-server-policy-test)#proxy retry-delay 8
RFController(config-radius-server-policy-test)#
```

## session-resumption

### *radius-server-policy*

Enables session resumption/fast reauthentication by using cached attributes

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
session-resumption {life-time|max-entries}
session-resumption life-time <1-24> {max-entries <10-1024>}
```

### Parameters

---

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {life-time max-entries <10-1024>} | <ul style="list-style-type: none"> <li>• life-time &lt;1-24&gt; - Sets the lifetime of cached entries             <ul style="list-style-type: none"> <li>• &lt;1-24&gt; - Sets the lifetime between 1 and 24 hours</li> </ul> </li> <li>• max-entries &lt;10-1024&gt; - Configures the maximum number of entries in the cache             <ul style="list-style-type: none"> <li>• &lt;10-1024&gt; - Sets the entries in the cache between 10 and 1024</li> </ul> </li> </ul> |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-radius-server-policy-test)#session-resumption lifetime 10
max-entries 11
RFController(config-radius-server-policy-test)#
```

## USE

### *radius-server-policy*

Defines settings used with the RADIUS Server policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
use [radius-group <RAD-GROUP> {RAD-GROUP}|radius-user-pool-policy
<RAD-USER-POOL>]
```

### Parameters

|                                            |                                                                                            |
|--------------------------------------------|--------------------------------------------------------------------------------------------|
| radius-group <RAD-GROUP><br>{RAD-GROUP}    | Configures a RADIUS group (for LDAP users). Specify a RADIUS group name to be used         |
| radius-user-pool-policy<br><RAD-USER-POOL> | Configures RADIUS user pool parameters. Specify a user name. It can be up to 32 characters |

### Example

```
RFController(config-radius-server-policy-test)#use server-trustpoint name1
RFController(config-radius-server-policy-test)#

RFController(config-radius-server-policy-test)#use radius-user-pool-policy
testuser
RFController(config-radius-server-policy-test)#
```

## radius-user-pool-policy

Configures a RADIUS User Pool policy.

Use the (config) instance to configure RADIUS User Pool Policy related configuration commands. To navigate to the radius-user-pool-policy instance, use the following commands.

```
RFController(config)#radius-user-pool-policy <pool name>
RFController(config)#radius-user-pool-policy testuser
RFController(config-radius-user-pool-testuser)#
```

[Table 40](#) Summarizes radius-user-pool-policy commands

**TABLE 40** radius-user-pool-policy commands

| Commands             | Description                                 | Reference                |
|----------------------|---------------------------------------------|--------------------------|
| <a href="#">user</a> | Configures RADIUS user parameters           | <a href="#">page 758</a> |
| <a href="#">no</a>   | Negates a command or sets its default value | <a href="#">page 758</a> |

## user

### *radius-user-pool-policy*

Configures RADIUS user parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
user <WORD> password [0|2|<WORD>] {group} RAD-GROUP {RAD-GROUP|guest}
user <WORD> password [0|2|<WORD>] {group} RAD-GROUP guest expiry-time <HH:MM>
expiry-date <MM:DD:YYY> {start-time}<HH:MM> start-date <MM:DD:YYYY>
```

### Parameters

---

|                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>&lt;WORD&gt; password 0 &lt;WORD&gt; {group} RAD-GROUP {RAD-GROUP guest expiry-time &lt;HH:MM&gt; expiry-date MM:DD:YYY {start-time} &lt;HH:MM&gt; start-date &lt;MM:DD:YYYY&gt;}</pre> | <p>Enter a RADIUS user name up to 64 characters</p> <ul style="list-style-type: none"> <li>• password [0 2 &lt;WORD&gt;] – Enter RADIUS user password <ul style="list-style-type: none"> <li>• 0 – Password is specified UNENCRYPTED</li> <li>• 2 – Password is specified ENCRYPTED</li> <li>• &lt;WORD&gt; – Enter password (specified UNENCRYPTED) up to 21 characters length <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Enter a RADIUS user password to configure. It can be up to 21 characters length <ul style="list-style-type: none"> <li>• {group} RAD-GROUP – Configures RADIUS server group configuration</li> <li>• RAD-GROUP – Specify an existing group name in the local database</li> <li>• guest – Enables guest user access</li> <li>• expiry-time &lt;HH:MM&gt; – Specify the expiry time for this user account in HH:MM format. For ex., 12:30 means 30 minutes after 12:00 the user login will expire</li> <li>• expiry-date &lt;MM:DD:YYYY&gt; – Specify time of expiry date for this user account in MM:DD:YYYY format. For ex. 12:15:2006</li> <li>• start-time &lt;HH:MM&gt; – Specify user activation time in HH:MM format</li> <li>• start-date &lt;MM:DD:YYYY&gt; – Specify user access start-date in MM:DD:YYYY format</li> </ul> </li> </ul> </li> </ul> </li> </ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-radius-user-pool-testuser)#user testuser password 0
admin123 group test guest expiry-time 13:20 expiry-
date 12:15:2010 start-time 17:00 start-date 11:15:2010
RFController(config-radius-user-pool-testuser)#
```

## no

*radius-user-pool-policy*

Negates a command or sets its default value

Supported in the following platforms:

### Syntaxs

```
no user <WORD>
```

### Parameters

---

|             |                                                |
|-------------|------------------------------------------------|
| user <WORD> | Deletes the existing RADIUS user configuration |
|-------------|------------------------------------------------|

---

### Example

```
RFController(config-radius-user-pool-testuser)#no user testuser  
RFController(config-radius-user-pool-testuser)#
```



# radio-qos-policy

## In this chapter

- [radio-qos-policy](#) ..... 759

This chapter summarizes the radio-qos-policy in detail.

Use the (config) instance to configure radio-qos-policy related configuration commands. To navigate to the radio-qos-policy instance, use the following commands:

```
RFController(config)#radio-qos-policy <policy-name>
RFController(config)#radio-qos-policy test
RFController(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
  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
RFController(config-radio-qos-test)#
```

## radio-qos-policy

[Table 41](#) Summarizes radio-qos-policy commands

**TABLE 41** radio-qos-policy commands

| Command                               | Description                                                                   | Reference                |
|---------------------------------------|-------------------------------------------------------------------------------|--------------------------|
| <a href="#">accelerated-multicast</a> | Configures multicast streams for acceleration                                 | <a href="#">page 760</a> |
| <a href="#">admission-control</a>     | Enables admission-control across all radios for one or more access categories | <a href="#">page 761</a> |
| <a href="#">no</a>                    | Negates a command or sets its default value                                   | <a href="#">page 763</a> |
| <a href="#">wmm</a>                   | Configures 802.11e/wireless multimedia parameters                             | <a href="#">page 764</a> |

## accelerated-multicast

### *radio-qos-policy*

Configures multicast streams for acceleration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
accelerated-multicast [client-timeout <5-6000>|max-client-streams
<1-4>|max-streams <0-256>|overflow-policy [reject|revert]|stream-threshold
<1-500>]
```

### Parameters

|                                 |                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-timeout <5-6000>         | Configure timeout for clients between 5 and 6000                                                                                                                                                         |
| max-client-streams<br><1-4>     | Configures maximum number of accelerated multicast streams per client. The default value is 2.                                                                                                           |
| max-streams <0-256>             | Configures maximum number of accelerated multicast streams per radio. The default value is 25.                                                                                                           |
| overflow-policy [reject revert] | Configures policy to follow in case too many clients register <ul style="list-style-type: none"> <li>• reject – Rejects new clients</li> <li>• revert – Reverts to regular multicast delivery</li> </ul> |
| stream-threshold <1-500>        | Configures packets per second for streams to accelerate. The default value is 30.                                                                                                                        |

### Example

```
RFController(config-radio-qos-test)#accelerated-multicast stream-threshold 15
RFController(config-radio-qos-test)#
```

## admission-control

### *radio-qos-policy*

Enables admission-control across all radios for one or more access categories

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
admission-control  
[background|best-effort|firewall-detected-traffic|implicit-tspec|video|voice]  
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

[background|best-effort|  
firewall-detected-traffic|  
implicit-tspec|video|voice]

- background – Configures background access category admissioncontrol parameters
- best-effort – Configures best effort access category admissioncontrol parameters
- video – Configures video access category admission-control parameters
- voice – Configures voice access category admission-control parameters

The following parameters are common for the above:

- max-airtime-percent<0-150> – Specifies the maximum percentage of airtime for this access category
  - <0-150> – Select a value between 0 and 150 to calculate the percentage of air-time (including oversubscription)
- max-clients – Specifies the maximum number of wireless clients admitted
  - <0-256> – Select the maximum number of wireless clients admitted to this access category
- max-roamed-clients <0-256> – Specifies the maximum number of roaming wireless clients admitted to this access category
  - <0-256> – Select the maximum number of roaming wireless devices admitted to this access category
- reserved-for-roam-percent <0-150> – Calculates the percentage of air time allocated exclusively for roamed wireless-clients. This value is calculated relative to the configured max air time for this access category
  - <0-150> – Select a value between 0 and 150 to calculate the percentage of air-time (including oversubscription)
- firewall-detected-traffic – Enforces admission control for traffic whose access category is detected by the firewall ALG (Eg: SIP voice calls)
- implicit-tspec – Enables implicit traffic-specifiers for clients that do not support WMM-TSPEC but are accessing admission controlled access categories

## Example

```
RFController(config-radio-qos-test)#admission-control best-effort max-mus 7
RFController(config-radio-qos-test)#
```

```
RFController(config-radio-qos-test)#admission-control voice
reserved-for-roam-percent 8
RFController(config-radio-qos-test)#
```

```
RFController(config-radio-qos-test)#admission-control voice
max-airtime-percent 9
RFController(config-radio-qos-test)#
```

## no

### *radio-qos-policy*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [accelerated-multicast | admission-control | wmm]
```

### Parameters

---

|                     |                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------|
| [admission-control] | • accelerated-multicast – Unconfigures multicast streams for acceleration                           |
| wmm]                | • admission-control – Unconfigures admission-control on the radio for one or more access categories |
|                     | • wmm – Unconfigures 802.11e/wireless multimedia parameters                                         |

---

### Example

```
RFController(config-radio-qos-test)#no admission-control best-effort enable
RFController(config-radio-qos-test)#
```

## wmm

### *radio-qos-policy*

Configures 802.11e/Wireless MultiMedia parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wmm [background|best-effort|video|voice] [aifsn <1-15>
|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```

### Parameters

[background|best-effort  
video|voice] [aifsn|cw-max|  
cw-min|txop-limit]

- background – Configures background access category parameters
- best-effort – Configures best effort access category parameters
- video – Configures video access category parameters
- voice – Configure voice access category parameters

The following parameters are common for all the above:

- aifsn <1-15> – Configures the arbitration inter frame spacing number (AIFSN) the wait time between data frames is derived from the AIFSN and slot-time
  - <1-15> – Select a value between 1 and 15 to configure the (AIFSN)
- cw-max <0-15> – Maximum contention window: 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
  - <0-15> – ECW: the contention window. The actual value used is  $(2^{ECW} - 1)$ . Sets a value from 0-15.
- cw-min – Minimum contention window: 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
  - <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)
  - <0-65535> – Select a value between 0 and 65535 to configure the transmit-opportunity in 32 microSecond units

**Example**

```
RFController(config-radio-qos-test)#wmm best-effort aifsn 7
RFController(config-radio-qos-test)#

RFController(config-radio-qos-test)#wmm voice txop-limit 1
RFController(config-radio-qos-test)#
```

---

**NOTE**

The commands `clrscr`, `commit`, `exit`, `end`, `help`, `write`, `revert`, `service` and `show` are common commands. For more information, see [Chapter 6, Common Commands](#).

---





## role-policy

---

### In this chapter

- [role-policy](#) ..... 767

This chapter summarizes Role Policies in detail.

Use the (config-role-policy) instance to configure role-policy related configuration commands. To navigate to the config-role instance, use the following commands:

```
RFController(config)#role-policy <policy-name>
RFController(config)#role-policy role1
RFController(config-role-policy-role1)# ?
Role Policy Mode commands:
  default-role  Configuration for Wireless Clients not matching any role
  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

RFController(config-role-policy-role1)#
```

## role-policy

[Table 42](#) Summarizes role-policy commands

**TABLE 42** role-policy commands

| Command                      | Description                                                                                     | Reference                |
|------------------------------|-------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">default-role</a> | When a client fails to find a matching role, the default-role action is assigned to that client | <a href="#">page 768</a> |
| <a href="#">no</a>           | Negates a command or sets its default value                                                     | <a href="#">page 769</a> |
| <a href="#">user-role</a>    | Creates a role and associates it to the newly created role policy                               | <a href="#">page 770</a> |

## default-role

### *role-policy commands*

When a client fails to find a matching role, the default role action is assigned to that client.

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
default-role use [ip-access-list|mac-access-list]
default-role use ip-access-list [in|out] <IP-ACCESS-LIST> precedence
<1-100>
default-role use mac-access-list [in|out] <MAC-ACCESS-LIST> precedence
<1-100>
```

### Parameters

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>use ip-access-list [in out] &lt;IP-ACCESS-LIST&gt; precedence &lt;1-100&gt;</pre>   | <p>Uses an IP access-list</p> <ul style="list-style-type: none"> <li>• in – Applies the rule to incoming packets</li> <li>• out – Applies the rule to outgoing packets</li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• &lt;IP-ACCESS-LIST&gt; – Specifies the access list name           <ul style="list-style-type: none"> <li>• precedence – Based on the packets received, the lower precedence value is evaluated first               <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specifies the precedence value between 1 and 100</li> </ul> </li> </ul> </li> </ul>                        |
| <pre>use mac-access-list [in out] &lt;MAC-ACCESS-LIST&gt; precedence &lt;1-100&gt;</pre> | <p>Uses a MAC access-list</p> <ul style="list-style-type: none"> <li>• in – Applies the rule to the incoming packets</li> <li>• out – Applies the rule to the outgoing packets</li> </ul> <p>The following parameters are common for the above:</p> <ul style="list-style-type: none"> <li>• &lt;MAC-ACCESS-LIST&gt; – Specifies the access-list name           <ul style="list-style-type: none"> <li>• precedence &lt;1-100&gt; – Based on the packets received, the lower precedence value is evaluated first               <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specifies the precedence value between 1 and 100</li> </ul> </li> </ul> </li> </ul> |

### Example

```
RFController(config-role-policy-test)#default-role use ip-access-list in test
precedence 1
RFController(config-role-policy-test)#

RFController(config-device-00-15-70-37-FA-BE)#show role wireless-clients on
RFController
Role: role1, precedence 1
No ROLE statistics found.
RFController(config-device-00-15-70-37-FA-BE)#
```

## no

### *role-policy commands*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [default-role|user-role]
```

### Parameters

|              |                             |
|--------------|-----------------------------|
| default-role | Deletes default role action |
| role         | Deletes a role              |

### Example

```
RFController(config-role-policy-test)#no default-role use ip-access-list in
test precedence 1
RFController(config-role-policy-test)#

RFController(config-role-policy-test)#show context
role-policy test
  role role1 precedence 1
RFController(config-role-policy-test)#
```

## user-role

### *role-policy commands*

Creates a role and associates it to the newly created role-policy

```
RFController(config-role-policy-test)#user- role <role-name> precedence
<1-10000>
RFController(config-role-policy-test)# user-role role1 precedence 1
RFController(config-role-role1)#
```

**Table 43** Summarizes role commands

**TABLE 43** user-role commands

| Commands                   | Description                                                 | Reference                |
|----------------------------|-------------------------------------------------------------|--------------------------|
| <i>ap-location</i>         | Sets the AP location                                        | <a href="#">page 771</a> |
| <i>authentication-type</i> | Selects authentication type for the role                    | <a href="#">page 772</a> |
| <i>captive-portal</i>      | Defines captive portal role based filter                    | <a href="#">page 773</a> |
| <i>encryption-type</i>     | Selects the encryption type                                 | <a href="#">page 774</a> |
| <i>group</i>               | Sets group configuration for the role                       | <a href="#">page 775</a> |
| <i>mu-mac</i>              | Configures the client MAC addresses for role based firewall | <a href="#">page 776</a> |
| <i>no</i>                  | Negates a command or sets its default values                | <a href="#">page 777</a> |
| <i>ssid</i>                | Specifies SSID configuration                                | <a href="#">page 778</a> |
| <i>use</i>                 | Defines the settings used with the role policy              | <a href="#">page 779</a> |

## *ap-location*

### *user-role commands*

Sets the AP location

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```

ap-location [any|contains|exact|not-contains]
ap-location any
ap-location contains <WORD>
ap-location exact <WORD>
ap-location not-contains <WORD>

```

### **Parameters**

|                     |                                                 |
|---------------------|-------------------------------------------------|
| any                 | Defines any AP location                         |
| contains <WORD>     | AP location contains the specified string       |
| exact <WORD>        | AP location contains the exact specified string |
| not-contains <word> | AP location does not contain the string         |

### **Example**

```

RFController(config-role-role1)#ap-location any
RFController(config-role-role1)#

RFController(config-role-role1)#ap-location contains office
RFController(config-role-role1)#

```

## *authentication-type*

### *user-role commands*

Selects the authentication type for the role

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```

authentication-type [any|eq|neq]
authentication-type any
authentication-type eq [eap|kerberos|mac-auth|none]
authentication-type neq[eap|kerberos|mac-auth|none]

```

### **Parameters**

|                                              |                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| any                                          | The authentication type can be any one from the listed options                                                                                                                                                                                                                                       |
| eq [eap kerberos <br>mac-auth none]          | The authentication type equals any one of the following types: <ul style="list-style-type: none"> <li>• eap – Extensible authentication protocol</li> <li>• kerberos – Kerberos authentication</li> <li>• mac-auth – MAC authentication protocol</li> <li>• none – no authentication used</li> </ul> |
| neq [eap hotspot kerberos <br>mac-auth none] | The authentication protocol does not contain one of the listed options                                                                                                                                                                                                                               |

### **Example**

```

RFController(config-role-role1)#authentication-type eq kerberos
RFController(config-role-role1)#

```

## *captive-portal*

### *user-role commands*

Defines captive portal based role filter

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
captive-portal authentication-state [any|post-login|pre-login]
```

### **Parameters**

---

|                                                    |                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authentication-state<br>[any post-login pre-login] | Defines authentication state of wireless client associated to captive portal <ul style="list-style-type: none"> <li>• any- Specifies any authentication state</li> <li>• post-login – Specifies authentication is completed successfully</li> <li>• pre-login – Specifies authentication is pending</li> </ul> |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```

RFController(config-role-policy-test-user-role-role1)#captive-portal
authentication-state pre-login
RFController(config-role-policy-test-user-role-role1)#

RFController(config-role-policy-test-user-role-role1)# show context
user-role role1 precedence 1
  captive-portal authentication-state pre-login
RFController(config-role-policy-test-user-role-role1)#

```

## *encryption-type*

### *user-role commands*

Selects the encryption type used for the role

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```

encryption-type [any|eq|neq]
encryption-type any
encryption-type eq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep64] {ccmp/keyguard/none/tkip/kip-ccmp/
wep128/wep64}
encryption-type neq [ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep64] {ccmp/keyguard/none/tkip/kip-ccmp/
wep128/wep64}

```

### **Parameters**

|                                           |                                                                                                                                                                                                                                                  |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| any                                       | The encryption type can be any one of the listed options                                                                                                                                                                                         |
| eq [ccmp keyguard none tkip wep128 wep64] | The encryption type equals one of the following: <ul style="list-style-type: none"> <li>• ccmp</li> <li>• keyguard</li> <li>• none</li> <li>• tkip</li> <li>• tkip-ccmp</li> <li>• wep128</li> <li>• wep128-keyguard</li> <li>• wep64</li> </ul> |
| neq[ccmp keyguard none tkip wep128 wep64] | The encryption type must not be one of the listed options                                                                                                                                                                                        |

### **Example**

```

RFController(config-role-role1)#encryption-type eq ccmp
RFController(config-role-role1)#

```



## *group*

### *user-role commands*

Sets the group configuration for the role

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
group [any|contains|exact|not-contains]
group any
group contains <WORD>
group exact <WORD>
group not-contains <WORD>
```

### **Parameters**

|                     |                                             |
|---------------------|---------------------------------------------|
| any                 | Specifies any group                         |
| contains <WORD>     | Group contains the specified string         |
| exact <WORD>        | Group contains the exact specified string   |
| not-contains <word> | Group does not contain the specified string |

### **Example**

```
RFController(config-role-role1)#group any
RFController(config-role-role1)#
```

***mu-mac****user-role commands*

Configures the client's MAC addresses for the role based firewall

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
mu-mac [<MAC Address> <Mask> <MAC Address> | any]
```

**Parameters**

|                      |                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <MAC Address>        | The address of the allowed client. The MAC address can be in the format AA-BB-CC-DD-EE-FF                                   |
| <MAC Address> <Mask> | The address and mask combination for the allowed client. <MAC Address> and <Mask> should be in the format AA-BB-CC-DD-EE-FF |
| any                  | Match with any MAC address                                                                                                  |

**Example**

```
RFController(config-role-role1)#mu-mac 11-22-33-44-55-66 mask
44-55-66-77-88-99 ?
```

```
RFController(config-role-role1)#mu-mac any
RFController(config-role-role1)#
```

## ***no***

### *user-role commands*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
no [ap-location|authentication-type|captive-portal|  
encryption-type|group|mu-mac|ssid|use]
```

### **Parameters**

None

### **Usage Guidelines**

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

### **Example**

```
RFController(config-role-policy-role1-user-role-role1)#no group  
RFController(config-role-policy-role1-user-role-role1)#  
  
RFController(config-role-policy-role1-user-role-role1)#no ap-location  
RFController(config-role-policy-role1-user-role-role1)#
```

***ssid******user-role commands***

Specifies the SSID configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
ssid [any|exact|contains|not-contains]
ssid [exact|contains|not-contains] <WORD>
```

**Parameters**


---

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [any exact contains not-contains] | <ul style="list-style-type: none"> <li>• any – Specifies that the SSID can be any value</li> <li>• contains &lt;WORD&gt; – Specifies SSID contains the given string</li> <li>• exact – Specifies SSID exactly matches with the given string</li> <li>• not-contains – Specifies SSID does not contain the given string           <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the string to match against - case sensitive (compared against SSID configured under WLAN)</li> </ul> </li> </ul> |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-role-policy-test-user-role-role1)#ssid not-contains
TESTSSID
RFController(config-role-policy-test-user-role-role1)#
```

**use**

*user-role commands*

Defines the settings used with the user role

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
use [ip-access-list|mac-access-list]
use ip-access-list [in|out] <IP-ACCESS-LIST> precedence
<1-100>
use mac-access-list [in|out] <MAC-ACCESS-LIST> precedence <1-100>
```

**Parameters**

---

|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip-access-list [in out]<br><IP-ACCESS-LIST> precedence<br><1-100>         | Uses an IP access list <ul style="list-style-type: none"> <li>• in – Applies the rule to incoming packets</li> <li>• out – Applies the rule to outgoing packets</li> </ul> The following parameters are common for the above: <ul style="list-style-type: none"> <li>• &lt;IP-ACCESS-LIST&gt; – Specifies the access list name                         <ul style="list-style-type: none"> <li>• precedence – Based on the packets received, the lower precedence value is evaluated first                                 <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specifies the precedence value between 1 and 100</li> </ul> </li> </ul> </li> </ul> |
| <hr/> mac-access-list [in out]<br><MAC-ACCESS-LIST> precedence<br><1-100> | Uses a MAC access list <ul style="list-style-type: none"> <li>• in – Applies the rule to incoming packets</li> <li>• out – Applies the rule to outgoing packets</li> </ul> The following parameters are common for the above: <ul style="list-style-type: none"> <li>• &lt;MAC-ACCESS-LIST&gt; – Specifies the access list name                         <ul style="list-style-type: none"> <li>• precedence – Based on the packets received, the lower precedence value is evaluated first                                 <ul style="list-style-type: none"> <li>• &lt;1-100&gt; – Specifies the precedence value is from 1 to 100</li> </ul> </li> </ul> </li> </ul> |

---

**Example**

```
RFController(config-role-role1)#use ip-access-list in test precedence 9
RFController(config-role-role1)#
```

**NOTE**

The commands no, write, clrscr, commit, exit, help, show, service are common commands. For more information, see [Chapter 6, Common Commands](#).



# smart-rf-policy

---

## In this chapter

- [smart-rf-policy](#) ..... 782

This chapter summarizes Smart-RF Policy commands within the CLI structure.

Use the (config) instance to configure Smart RF Policy related configuration commands. To navigate to the smart-rf-policy instance, use the following commands:

```
RFController(config)#smart-rf-policy <policy name>
RFController(config)#smart-rf-policy test
RFController(config-smart-rf-policy-test)#?
Smart RF Mode commands:
  assignable-power      Specify the assignable power during power-assignment
  auto-assign-sensor    Allow smart-rf to select optimal sensor radios for
                        wips and unauthorized ap detection
  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

RFController(config-smart-rf-policy-test)#
```

## smart-rf-policy

Table 44 Summarizes Smart RF Policy commands

**TABLE 44** smart-rf-policy commands

| Command                                | Description                                                                            | Reference                |
|----------------------------------------|----------------------------------------------------------------------------------------|--------------------------|
| <a href="#">assignable-power</a>       | Specifies the power range during power assignment                                      | <a href="#">page 783</a> |
| <a href="#">auto-assign-sensor</a>     | Allows Smart RF to select optimal sensor radios for WIPS and unauthorized AP detection | <a href="#">page 784</a> |
| <a href="#">channel-list</a>           | Assigns the channel list for the selected frequency                                    | <a href="#">page 785</a> |
| <a href="#">channel-width</a>          | Selects the channel width for Smart RF configuration                                   | <a href="#">page 786</a> |
| <a href="#">coverage-hole-recovery</a> | Enables recovery from coverage-hole errors                                             | <a href="#">page 787</a> |
| <a href="#">enable</a>                 | Enables the configured Smart RF Policy settings                                        | <a href="#">page 788</a> |
| <a href="#">group-by</a>               | Configures grouping parameters                                                         | <a href="#">page 789</a> |
| <a href="#">interference-recovery</a>  | Recovers issues due to excessive noise and interference                                | <a href="#">page 790</a> |
| <a href="#">neighbor-recovery</a>      | Enables recovery from errors due to faulty neighbor radios                             | <a href="#">page 791</a> |
| <a href="#">no</a>                     | Negates a command or sets its default values                                           | <a href="#">page 792</a> |
| <a href="#">sensitivity</a>            | Configures Smart RF sensitivity                                                        | <a href="#">page 793</a> |
| <a href="#">smart-ocs-monitoring</a>   | Applies smart off channel scanning instead of dedicated detectors                      | <a href="#">page 794</a> |



## assignable-power

### *smart-rf-policy*

Specifies the power range during power assignment

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
assignable-power [2.4Ghz|5Ghz] [max|min] <1-20>
```

### Parameters

---

|                                   |                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [2.4Ghz 5Ghz] [max min]<br><1-20> | [2.4Ghz 5Ghz] [max min] <1-20> – Specifies the power range during power assignment <ul style="list-style-type: none"><li>• max &lt;1-20&gt; – Sets the upper bound of the power range. The value is between 1 and 20</li><li>• min &lt;1-20&gt; – Sets the lower bound of the power range. The value is between 1 and 20</li></ul> |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-smart-rf-policy-test)#assignable-power 5Ghz min 8  
RFController(config-smart-rf-policy-test)#
```

### auto-assign-sensor

#### *smart-rf-policy commands*

Allows Smart RF to select optimal sensor radios for WIPS and unauthorized AP detection

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

#### **Parameters**

None

#### **Example**

```
RFController(config-smart-rf-policy-test)#auto-assign-sensor
RFController(config-smart-rf-policy-test)#
```

## channel-list

### *smart-rf-policy*

Assigns the channel list for the selected frequency

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
channel-list [2.4Ghz|5Ghz] <WORD>
```

### Parameters

---

|                      |                                                      |
|----------------------|------------------------------------------------------|
| [2.4Ghz 5Ghz] <WORD> | Assigns the channel list for the selected frequency  |
|                      | • <WORD> - A comma separated list of channel numbers |

---

### Example

```
RFController(config-smart-rf-policy-test)#channel-list 2.4Ghz 1,12
RFController(config-smart-rf-policy-test)#
```

## channel-width

### *smart-rf-policy*

Selects the channel width for Smart RF configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
channel-width [2.4Ghz|5Ghz] [20Mhz|40Mhz|auto]
```

### Parameters

---

|                    |                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [2.4Ghz 5Ghz]      | Assigns the channel width for the selected frequency                                                                                                                                                                     |
| [20Mhz 40Mhz auto] | <ul style="list-style-type: none"> <li>• 20Mhz - Assigns the 20Mhz channel width</li> <li>• 40Mhz - Assigns the 40Mhz channel width</li> <li>• auto - Assigns the best possible channel in the 20/40Mhz width</li> </ul> |

---

### Example

```
RFController(config-smart-rf-policy-test)#channel-width 5 auto
RFController(config-smart-rf-policy-test)#
```

```
RFController(config-smart-rf-policy-test)#channel-width 5 40Mhz
RFController(config-smart-rf-policy-test)#
```

## coverage-hole-recovery

### *smart-rf-policy*

Enables recovery from coverage hole errors

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### 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

- 
- |                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| client-threshold coverage-interval interval snr-threshold} | <ul style="list-style-type: none"> <li>• client-threshold &lt;1-255&gt; – Specifies the minimum number of clients below SNR threshold required for coverage hole recovery. Select the number of cents between 1 and 255.</li> <li>• coverage-interval &lt;1-120&gt; – Specify the interval at which recovery should be performed after coverage hole is discovered. Select a interval coverage-interval value between 1 and 120 seconds</li> <li>• interval &lt;1-120&gt; – Specify the interval at which a coverage hole recovery should be performed before coverage hole is detected. Select a interval value between 1 and 120 seconds</li> <li>• snr-threshold &lt;1-75&gt; – Specify the SNR threshold below which coverage recovery is initiated. Select a SNR threshold value between 1 and 75</li> </ul> |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The following bandwidth is common for all the above:

- 2.4GHz – 2.4GHz band
  - 5GHz – 5GHz band
- 

### Example

```
RFController(config-smart-rf-policy-test)#coverage-hole-recovery
snr-threshold 5Ghz 1
```

```
RFController(config-smart-rf-policy-test)#
```

## enable

### *smart-rf-policy*

Enables the configured Smart RF policy settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
enable
```

### Parameters

None

### Example

```
RFController(config-smart-rf-policy-test)#enable
RFController(config-smart-rf-policy-test)#

RFController(config-smart-rf-policy-test)#show context
smart-rf-policy test
  enable
  calibration wait-time 4
RFController(config-smart-rf-policy-test)#
```

## group-by

### *smart-rf-policy commands*

Configures grouping parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
group-by [building|floor]
```

### Parameters

---

|                  |                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| [building floor] | <ul style="list-style-type: none"><li>• building – Configures a group based on building</li><li>• floor – Configures a group based on floor</li></ul> |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-smart-rf-policy-test)#group-by floor
RFController(config-smart-rf-policy-test)#
```

## interference-recovery

### smart-rf-policy

Recovers detected problems due to excessive noise and interference

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
interference-recovery {channel-hold-time <0-86400> |channel-switch-delta
[2.4Ghz|5Ghz] <5-35>|client-threshold <1-255>|interference|noise}
```

### Parameters

|                                              |                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel-hold-time <0-86400>                  | <p>Defines the minimum time between two channel change recoveries</p> <ul style="list-style-type: none"> <li>• &lt;0-86400&gt; – Sets the time between channel assignments based on interference/noise in seconds</li> </ul>                                                                                                |
| channel-switch-delta<br>[2.4Ghz 5Ghz] <5-35> | <p>Specifies the difference between the current and best channel interference for a channel change</p> <ul style="list-style-type: none"> <li>• 2.4Ghz 5Ghz &lt;5-35&gt; – Select the band width as 2.4Ghz or 5Ghz</li> <li>• &lt;5-35&gt; – Specify the difference in dbm by selecting a value between 5 and 35</li> </ul> |
| interference                                 | Considers the external interference values for performing interference recovery                                                                                                                                                                                                                                             |
| noise                                        | Considers the noise values for performing interference recovery                                                                                                                                                                                                                                                             |
| client-threshold <1-255>                     | <p>Specifies client thresholds associated after which, a channel change due to interference recovery is avoided</p> <ul style="list-style-type: none"> <li>• &lt;1-255&gt; – Specify the number of clients between 1 and 255</li> </ul>                                                                                     |

### Example

```
RFController(config-smart-rf-policy-test)#interference-recovery
channel-switch-delta 5 5
RFController(config-smart-rf-policy-test)#

RFController(config-smart-rf-policy-test)#interference-recovery interference
RFController(config-smart-rf-policy-test)#

RFController(config-smart-rf-policy-test)#interference-recovery
retry-threshold 0.9
RFController(config-smart-rf-policy-test)#
```



## neighbor-recovery

### *smart-rf-policy*

Enables a recovery from errors due to faulty neighbor radios

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
neighbor-recovery {power-hold-time <0-3600>/power-threshold} [2.4Ghz|5Ghz]
<-85--55>
```

### Parameters

|                                          |                                                                                                                                                                                                                                                                      |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| power-hold-time <0-3600>                 | Specifies the minimum time between two power change recoveries <ul style="list-style-type: none"> <li>• &lt;0-3600&gt; - Sets the time between 0 and 3600 seconds</li> </ul>                                                                                         |
| {power-threshold} [2.4Ghz 5Ghz] <-85-55> | Specifies the power threshold based on the recovery performed <ul style="list-style-type: none"> <li>• 2.4Ghz 5Ghz &lt;-85-55&gt; - Select the band width as 2.4 Ghz or 5Ghz</li> <li>• &lt;-85-55&gt; - Select a threshold value between -85 and -55 dbm</li> </ul> |

### Example

```
RFController(config-smart-rf-policy-test)#neighbor-recovery power-threshold
2.4 -82
RFController(config-smart-rf-policy-test)#

RFController(config-smart-rf-policy-test)#neighbor-recovery power-threshold 5
-65
RFController(config-smart-rf-policy-test)#
```

## no

### *smart-rf-policy*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [assignable-power|auto-assign|calibration|
channel-list|channel-width|coverage-hole-recovery|enable|
group-by|interference-recovery|neighbor-recovery|
smart-ocs-monitoring]
```

### Parameters

---

|                               |                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------|
| [assignable-power]            | • assignable-power – Negates the power range assignment                                       |
| auto-assign calibration]      | • auto-assign – Disables all auto assignment features                                         |
| channel-list]                 | • calibration – Resets calibration parameters                                                 |
| channel-width]                | • channel-list – Removes the assigned channel-list for the selected frequency                 |
| coverage-hole-recovery enable | • channel-width – Removes the assigned channel-width for the selected frequency               |
| hold-time                     | • coverage-hole-recovery – Disables recovery from coverage hole errors                        |
| interference-recovery         | • enable – Disables the Smart RF policy feature                                               |
| neighbor-recovery             | • group-by – Unconfigures grouping parameters                                                 |
| smart-ocs-monitoring]         | • interference-recovery – Disables recovery issues caused by excessive noise and interference |
|                               | • neighbor-recovery – Disables recovery issues caused by faulty neighbor radios               |
|                               | • smart-ocs-monitoring – Disables the off channel monitoring feature                          |

---

### Example

```
RFController(config-smart-rf-policy-test)#no assignable-power 5Ghz min
RFController(config-smart-rf-policy-test)#
```

```
RFController(config-smart-rf-policy-test)#no smart-ocs-monitoring frequency
2.4Ghz
RFController(config-smart-rf-policy-test)#
```

## sensitivity

### *smart-rf-policy*

Configures Smart-RF sensitivity

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
sensitivity [custom|high|low|medium]
```

### Parameters

---

|                          |                                                                                                                                                                                                                       |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [custom high low medium] | Configures Smart-RF sensitivity <ul style="list-style-type: none"><li>• Custom – Custom sensitivity</li><li>• high – High sensitivity</li><li>• low – low sensitivity</li><li>• medium – Medium sensitivity</li></ul> |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-smart-rf-policy-test)#sensitivity medium
RFController(config-smart-rf-policy-test)#
```

## smart-ocs-monitoring

### *smart-rf-policy*

Applies smart off channel scanning instead of dedicated detectors

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
smart-ocs-monitoring {extended-scan-frequency|frequency|
off-channel-duration|sample-count}
```

### Parameters

---

|                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{extended-scan-frequency frequency  off-channel-duration  sample-count}</pre> | <ul style="list-style-type: none"> <li>• extended-scan-frequency [2.4Ghz 5Ghz] &lt;0-50&gt; – Specifies the frequency at which an extended scan is performed instead of a neighbor only scan. Sets the number of trails from 0-50.</li> <li>• frequency [2.4Ghz 5Ghz] &lt;1-120&gt; – Specifies the frequency at which the channel has to be switched. Sets the value in seconds from 1-120.</li> <li>• off-channel-duration [2.4Ghz 5Ghz] &lt;20-150&gt; – Specifies the duration required to spend off channel. Sets the value in milliseconds from 20-150</li> <li>• sample-count [2.4Ghz 5Ghz] &lt;1-120&gt; – Specifies the number of samples collected before reporting to the Smart-RF master. Sets the sample-count from 1-120.</li> </ul> |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-smart-rf-policy-test)#smart-ocs-monitoring
extended-scan-frequency 2.4Ghz 9
RFController(config-smart-rf-policy-test)#

RFController(config-smart-rf-policy-test)#smart-ocs-monitoring sample-count
2.4Ghz 3
RFController(config-smart-rf-policy-test)#

RFController(config-smart-rf-policy-test)#smart-ocs-monitoring
off-channel-duration 2.4Ghz 25
RFController(config-smart-rf-policy-test)#
```

### NOTE

The commands `clear`, `commit`, `end`, `exit`, `help`, `revert`, `service`, `show`, `write` are common commands across all chapters. For more information, see [Chapter 6, Common Commands](#).

---

## wips-policy

## In this chapter

- [wips-policy](#) ..... 796

This chapter summarizes WIPS-Policy in detail.

Use the (config) instance to configure wips-policy related configuration commands. To navigate to the WIPS-Policy instance, use the following commands:

```
RFController(config)#wips-policy <policy-name>
RFController(config)#wips-policy test
RFController(config-wips-policy-test)#?
Wips Policy Mode commands:
  ap-detection           Unsanctioned AP detection
  enable                 Enable this wips policy
  event                  Configure an event
  history-throttle-duration
  are not stored in history
  history-throttle-duration
  Configure the duration for which event duplicates
  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

RFController(config-wips-policy-test)#
```

## wips-policy

[Table 45](#) Summarizes WIPS-Policy commands in detail

**TABLE 45** wips-policy commands

| Command                                   | Description                                                        | Reference                |
|-------------------------------------------|--------------------------------------------------------------------|--------------------------|
| <a href="#">ap-detection</a>              | Defines ap-detection configuration                                 | <a href="#">page 797</a> |
| <a href="#">enable</a>                    | Enables wips-policy                                                | <a href="#">page 798</a> |
| <a href="#">event</a>                     | Configures events                                                  | <a href="#">page 799</a> |
| <a href="#">history-throttle-duration</a> | Configures the duration event duplicates are not stored in history | <a href="#">page 802</a> |
| <a href="#">use</a>                       | Defines the settings used with the WIPS policy                     | <a href="#">page 804</a> |
| <a href="#">no</a>                        | Negates a command or sets its default values                       | <a href="#">page 803</a> |
| <a href="#">signature</a>                 | Configures signature                                               | <a href="#">page 805</a> |

## ap-detection

### *wips-policy*

Defines ap-detection configuration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
ap-detection {age-out <30-86400>/wait-time <10-600>}
```

### Parameters

|                    |                                                      |
|--------------------|------------------------------------------------------|
| age-out <30-86400> | Configures the age out time between 30-86400 seconds |
| wait-time <10-600> | Configures the wait time between 10-600 seconds      |

### Example

```
RFController(config-wips-policy-test)#ap-detection wait-time 15
RFController(config-wips-policy-test)#

RFController(config-wips-policy-test)#ap-detection age-out 50
RFController(config-wips-policy-test)#
```

## enable

*wips-policy*

Enables wips-policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
enable
```

### Parameters

---

|        |                       |
|--------|-----------------------|
| enable | Enables a WIPS policy |
|--------|-----------------------|

---

### Example

```
RFController(config-wips-policy-test)#enable
RFController(config-wips-policy-test)#
```



## event

### *wips-policy*

Configures an event

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
event [ap-anomaly|client-anomaly|enable-all-events|excessive]
```

```
event ap-anomaly [ad-hoc-advertise-authorized-ssid |
ad-hoc-violation|airjack|ap-default-config|ap-ssid-broadcast-in-beacon|asleep
|fake-ap-flood|impersonation-attack|null-probe-response|suspicious-ap-high-rs
si|transmitting-device-using-invalid-mac|unauthorized-ap-using-authorized-ssi
d|unencrypted-wired-leakage|wireless-bridge]
```

```
event client-anomaly
[crackable-wep-iv-key-usedr|dos-broadcast-death|frames-with-bad-essids|fuzzi
ng-all-zero-macs|fuzzing-invalid-frame-type|fuzzing-invalid-mgmt-frames|fuzzi
ng-invalid-seq-num|identical-src-and-dest-addr|invalid-8021x-frames|
netstumbler-generic|
non-changing-wep-iv|tkip-mic-counter-measures|wellenreiter]
{filter-ageout <0-86400>}]
```

```
event excessive [80211-replay-check-failure|
aggressive-scanning|auth-server-failures|decryption-failures|dos-assoc-or-aut
h-flood|dos-eapol-start-storm
|dos-unicast-death-or-disassoc|eap-flood|eap-nak-flood
|frames-from-unassoc-station|replay-injection-attack] {filter-ageout
<0-86400>|threshold-clientmu <0-65535> |threshold-radio <0-65535>}
```

## Parameters

|                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ap-anomaly [  <br>ad-hoc-violation  airjack  <br>ap-ssid-broadcast-in-beacon  asle<br>ap  impersonation-attack  <br>null-probe-response  <br>transmitting-device-using-invalid-m<br>ac  <br>unencrypted-wired-leakage  wirele<br>ss-bridge]                                                                                                                                               | Configures ap-anomaly type events <ul style="list-style-type: none"> <li>• ad-hoc-violation – Ad-Hoc network violation</li> <li>• airjack – AirJack attack</li> <li>• ap-ssid-broadcast-in-beacon – AP SSID broadcast in beacon</li> <li>• asleep – ASLEAP attack</li> <li>• impersonation-attack – Impersonation attack detected</li> <li>• null-probe-response – Null probe response</li> <li>• transmitting-device-using-invalid-mac – Transmitting device using invalid MAC</li> <li>• unencrypted-wired-leakage – Unencrypted wired leakage detected</li> <li>• wireless-bridge – Wireless Bridge (WDS) frames detected</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| client-anomaly[crackable-wep-iv-k<br>ey-used   dos-broadcast-deauth  <br>fuzzing-all-zero-macs  fuzzing-invali<br>d-frame-type  <br>fuzzing-invalid-mgmt-frames  <br>fuzzing-invalid-seq-num  identical-<br>src-and-dest-addr  <br>invalid-8021x-frames  <br>netstumbler-generic  <br>non-changing-wep-iv  tkip-mic-cou<br>nter-measures  wellenreiter<br>] {filter-agetimeout <0-86400>} | Configures client-anomaly type events <ul style="list-style-type: none"> <li>• crackable-wep-iv-key-used – Crackable WEP IV Key Used</li> <li>• dos-broadcast-deauth – DoS broadcast deauthentication</li> <li>• fuzzing-all-zero-macs – Fuzzing: All zero MAC address observed</li> <li>• fuzzing-invalid-frame-type – Fuzzing:invalid frame type detected</li> <li>• fuzzing-invalid-mgmt-frames – Fuzzing: invalid management frame</li> <li>• fuzzing-invalid-seq-num – Fuzzing: invalid sequence number</li> <li>• identical-src-and-dest-addr – Identical source and destination addresses</li> <li>• invalid-8021x-frames – Fuzzing: Invalid 802.1x frames detected</li> <li>• netstumbler-generic – Netstumbler (v3.2.0, 3.2.3, 3.3.0)</li> <li>• non-changing-wep-iv – Non-changing WEP IV</li> <li>• tkip-mic-counter-measures – TKIP MIC counter measures caused by station</li> <li>• wellenreiter – Wellenreiter</li> </ul> <p>The following parameters are common for all the above:</p> <ul style="list-style-type: none"> <li>• {filter-ageout &lt;0-86400&gt;} – Configures filter-ageout             <ul style="list-style-type: none"> <li>• &lt;0-86400&gt; – Configures filter-ageout values between 0 and 86400 seconds</li> </ul> </li> </ul>                                                                                                                                                                                                                 |
| enable-all-events                                                                                                                                                                                                                                                                                                                                                                         | Enables all events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| excessive<br>[ 80211-replay-check-failure  <br>aggressive-scanning   auth-server-f<br>ailures  <br>decryption-failures   dos-assoc-or-a<br>uth-flood   dos-eapol-start-storm  <br>dos-unicast-deauth-or-disassoc  e<br>ap-flood   eap-nak-flood<br>  frames-from-unassoc-station ]<br>{filter-ageout<br><0-86400>   threshold-mu<br><0-65535><br>  thr eshold-radio <0-65535>             | Configures excessive type events <ul style="list-style-type: none"> <li>• 80211-replay-check-failure – 802.11replay check failure</li> <li>• aggressive-scanning – Aggressive scanning</li> <li>• auth-server-failures – Failures reported by authentication servers</li> <li>• decryption-failures – Decryption failures</li> <li>• dos-assoc-or-auth-flood – DoS association or authentication flood</li> <li>• dos-eapol-start-storm – DoS EAPOL-start storm</li> <li>• dos-unicast-deauth-or-disassoc – DoS association or authentication flood</li> <li>• eap-flood – EAP flood</li> <li>• eap-nak-flood – EAP-NAK flood</li> <li>• frames-from-unassoc-station – Frames from unassociated stations</li> </ul> <p>The following parameters are common for all the above:</p> <ul style="list-style-type: none"> <li>• {filter-ageout &lt;0-86400&gt;} – Configures filter-ageout             <ul style="list-style-type: none"> <li>• &lt;0-86400&gt; – Configures filter-ageout values between 0 and 86400 seconds</li> </ul> </li> <li>• threshold-client &lt;0-65535&gt; – Configures threshold-client             <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Configures wireless client threshold limit for 60 seconds</li> </ul> </li> <li>• threshold-radio &lt;0-65535&gt; – Configures Radio threshold configuration             <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Radio threshold limit for 60 seconds</li> </ul> </li> </ul> |

**Example**

```
RFController(config-wips-policy-test)#event enable-all-events
RFController(config-wips-policy-test)#
RFController(config-wips-policy-test)#event excessive
80211-replay-check-failure filter-ageout 9 threshold-clientmu 8
threshold-radio 99
RFController(config-wips-policy-test)#

RFController(config-wips-policy-test)#event client-anomaly wellenreiter
filter-ageout 99
RFController(config-wips-policy-test)#
```

## history-throttle-duration

### *wips-policy*

Configures the duration where event duplicates are not stored in the history

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
history-throttle-duration <30-86400>
```

### Parameters

---

|                                         |                                                                        |
|-----------------------------------------|------------------------------------------------------------------------|
| history-throttle-duration<br><30-86400> | Configures the duration event duplicates are not stored in the history |
|                                         | • <30-86400> - Configures the duration in seconds                      |

---

### Example

```
RFController(config-wips-policy-test)#history-throttle-duration 77
RFController(config-wips-policy-test)#
```

## no

### *wips-policy*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
no [ap-detection|enable|evbent|history-throttle-duration|signature|use]
```

### Parameters

None

### Usage Guidelines

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

### Example

```
RFController(config-wips-policy-test)#no enable
RFController(config-wips-policy-test)#

RFController(config-wips-policy-test)#no ap-detection
RFController(config-wips-policy-test)#

RFController(config-wips-policy-test)#no event ap-anomaly
ad-hoc-advertise-authorized-ssid
RFController(config-wips-policy-test)#

RFController(config-wips-policy-test)#no history-throttle-duration
RFController(config-wips-policy-test)#
```

## USE

### *wips-policy*

Defines the settings used with the WIPS policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 650 Access Point
- Mobility 7131 Series Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
use device-categorization <DEVICE-CATEGORIZATION>
```

### Parameters

---

|                                                  |                                                                                                                                                                                                                |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| device-categorization<br><DEVICE-CATEGORIZATION> | Configures the device categorization list <ul style="list-style-type: none"> <li>• &lt;DEVICE-CATEGORIZATION&gt; - Specify the device categorization object name to be associated with this profile</li> </ul> |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wips-policy-test)#use device-categorization rfs7000
RFController(config-wips-policy-test)#

RFController(config-wips-policy-test)#show context
wips-policy test
  no enable
  signature test
    src-mac 11-22-33-44-55-66
  signature testsignature
  ap-detection-ageout 35
  ap-detection-wait-time 15
  use device-categorization rfs7000
RFController(config-wips-policy-test)#
```

## signature

### *wips-policy*

Defines the signature

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 650 Access Point
- Mobility 7131 Series Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
signature <signature-name>
```

### Parameters

---

|                            |                                                                  |
|----------------------------|------------------------------------------------------------------|
| signature <signature-name> | Configures signature                                             |
|                            | • <signature-name> - Specify the signature name to be configured |

---

### Example

```
RFController(config-wips-policy-test)#signature brocade
RFController(config-test-signature-brocade)#
```

---

### NOTE

Please refer to [signature commands](#) for signature-mode related commands.

---

Table 46 Summarizes signature commands

**TABLE 46** signature commands

| <b>Commands</b>         | <b>Description</b>                             | <b>Reference</b>         |
|-------------------------|------------------------------------------------|--------------------------|
| <i>ssid</i>             | Configures ssid MAC address                    | <a href="#">page 807</a> |
| <i>dst-mac</i>          | Configures destination MAC address             | <a href="#">page 808</a> |
| <i>filter-ageout</i>    | Configures filter-ageout                       | <a href="#">page 809</a> |
| <i>frame-type</i>       | Configures frame-type to match                 | <a href="#">page 810</a> |
| <i>mode</i>             | Enables/Disables signature mode                | <a href="#">page 811</a> |
| <i>payload</i>          | Configures payload settings                    | <a href="#">page 812</a> |
| <i>src-mac</i>          | Configures source MAC address                  | <a href="#">page 813</a> |
| <i>ssid-match</i>       | Configures the match based on SSID             | <a href="#">page 814</a> |
| <i>threshold-client</i> | Configures the wireless client threshold limit | <a href="#">page 815</a> |
| <i>threshold-radio</i>  | Configures radio threshold limit               | <a href="#">page 816</a> |
| <i>no</i>               | Negates a command or sets its default values   | <a href="#">page 817</a> |



## *bssid*

### *signature commands*

Configures BSSID MAC address

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
bssid <MAC Address>
```

### **Parameters**

---

|                     |                                                    |
|---------------------|----------------------------------------------------|
| bssid <MAC Address> | Configures BSSID MAC address                       |
|                     | • <MAC Address> - Specify the MAC address to match |

---

### **Example**

```
RFController(config-test-signature-brocade)#bssid 11-22-33-44-55-66  
RFController(config-test-signature-brocade)#
```

## *dst-mac*

### *signature commands*

Configures destination MAC address

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
dst-mac <MAC Address>
```

### **Parameters**

---

|                       |                                                    |
|-----------------------|----------------------------------------------------|
| dst-mac <MAC Address> | Configures destination MAC address                 |
|                       | • <MAC Address> - Specify the MAC address to match |

---

### **Example**

```
RFController(config-test-signature-brocade)#dst-mac 11-22-33-44-55-66  
RFController(config-test-signature-brocade)#
```

## *filter-ageout*

### *signature commands*

Configures the filter ageout in seconds

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
filter-ageout <1-86400>
```

### **Parameters**

---

|                         |                                                    |
|-------------------------|----------------------------------------------------|
| filter-ageout <1-86400> | Configures filter-ageout                           |
|                         | • <1-86400> - Specify the filter-ageout in seconds |

---

### **Example**

```
RFController(config-test-signature-brocade)#filter-ageout 8  
RFController(config-test-signature-brocade)#
```

## *frame-type*

### *signature commands*

Configures frame-type to match

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
frame-type [all|assoc|auth|beacon|data|deauth|disassoc|
           mgmt|probe-req|probe-resp|reassoc]
```

### **Parameters**

---

|                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frame-type [ all assoc <br>auth beacon data <br>deauth disassoc mgmt <br>probe-req <br>probe-resp reassoc] | Configures frame type to match from the list <ul style="list-style-type: none"> <li>• all – Configures association frames</li> <li>• assoc – Authentication frames</li> <li>• auth – Beacon frames</li> <li>• beacon – Control frames</li> <li>• data – Data frames</li> <li>• deauth – Deauthentication frames</li> <li>• disassoc – Disassociation frames</li> <li>• mgmt – Management frames</li> <li>• probe-req – Probe request frames</li> <li>• probe-resp – Probe response frames</li> <li>• reassoc – Reassociation frames</li> </ul> |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-test-signature-brocade)#frame-type reassoc
RFController(config-test-signature-brocade)#
RFController(config-test-signature-brocade)#frame-type all
RFController(config-test-signature-brocade)#
```

## *mode*

### *signature commands*

Enables/Disables signature mode

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
mode enable
```

### **Parameters**

---

|             |                                 |
|-------------|---------------------------------|
| mode enable | Enables/Disables signature mode |
|-------------|---------------------------------|

---

### **Example**

```
RFController(config-test-signature-brocade)#enable  
RFController(config-wips-policy-test)#
```

## *payload*

### *signature commands*

Configures the payload settings

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
payload <1-3> pattern <WORD> offset <0-255>
```

### **Parameters**

---

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| payload <1-3> pattern | <p>Configures the payload settings</p> <ul style="list-style-type: none"> <li>• &lt;1-3&gt; pattern – Specify the payload index</li> <li>• &lt;pattern&gt; &lt;WORD&gt; – Specify the pattern to match hex or string <ul style="list-style-type: none"> <li>• &lt;WORD&gt; – Specify the pattern name <ul style="list-style-type: none"> <li>• offset &lt;0-255&gt; – Sets the offset in the payload to start the pattern match</li> <li>• &lt;0-255&gt; – Specify the offset value</li> </ul> </li> </ul> </li> </ul> |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-test-signature-brocade)#payload 1 pattern brocade offset 1
RFController(config-test-signature-brocade)#
```

## *src-mac*

### *signature commands*

Configures source MAC address

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
src-mac <MAC Address>
```

### **Parameters**

---

|                       |                                                           |
|-----------------------|-----------------------------------------------------------|
| src-mac <MAC Address> | Configures source MAC address                             |
|                       | • <MAC Address> - Specify the source MAC address to match |

---

### **Example**

```
RFController(config-test-signature-brocade)#src-mac 00-1E-E5-EA-1D-60  
RFController(config-test-signature-brocade)#
```

***ssid-match****signature commands*

Configures the match based on SSID

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
ssid-match [ssid<WORD>|ssid-len <0-32> ]
```

**Parameters**


---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssid-match [ssid ssid-len] | <p>Configures the match based on the SSID</p> <ul style="list-style-type: none"> <li>• ssid &lt;WORD&gt; - Specify the SSID string match             <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify the SSID to match</li> </ul> </li> <li>• ssid-len &lt;0-32&gt; - Specify the SSID length match             <ul style="list-style-type: none"> <li>• &lt;0-32&gt; - Specify the SSID character length</li> </ul> </li> </ul> |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-test-signature-brocade)#ssid-match ssid dell
RFController(config-test-signature-brocade)#
```



## *threshold-client*

### *signature commands*

Configures the wireless client threshold limit

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
threshold-clientmu <0-65535>
```

### **Parameters**

---

|                               |                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| threshold-client<br><1-65535> | Configures the wireless client threshold limit <ul style="list-style-type: none"><li>• &lt;1-65535&gt; - Specify the threshold value for a 60 second window between 1 and 65535</li></ul> |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-test-signature-brocade)#threshold-muclient 88  
RFController(config-test-signature-brocade)#
```

***threshold-radio******signature commands***

Configures radio threshold limit

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
threshold-radio <1-65535>]
```

**Parameters**


---

|                              |                                                                                                                                                                                   |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| threshold-radio<br><1-65535> | Configures the radio threshold limit <ul style="list-style-type: none"> <li>• &lt;1-65535&gt; - Specify the threshold value for a 60 second window between 1 and 65535</li> </ul> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-test-signature-brocade)#threshold-mu 88
RFController(config-test-signature-brocade)#
RFController(config-test-signature-brocade)#threshold-radio 88
RFController(config-test-signature-brocade)#
```

## ***no***

### *signature commands*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### **Syntax**

```
no [bssid|dts-mac|filter-ageout|frame-type|mode|payload|src-mac|  
ssid-match|threshold-client|threshold-radio]
```

### **Parameters**

None

### **Usage Guidelines**

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

### **Example**

```
RFController(config-test-signature-signature1)#no bssid  
RFController(config-test-signature-signature1)#  
  
RFController(config-test-signature-signature1)#no dst-mac  
RFController(config-test-signature-signature1)#  
  
RFController(config-test-signature-signature1)#no filter-ageout  
RFController(config-test-signature-signature1)#  
  
RFController(config-test-signature-signature1)#no threshold-radio  
RFController(config-test-signature-signature1)#
```



## wlan-qos-policy

---

### In this chapter

- [wlan-qos-policy](#) ..... 820

This chapter summarizes the WLAN QoS Policy in detail.

Use the (config) instance to configure WLAN QoS Policy related configuration commands. To navigate to the WLAN QoS Policy instance, use the following commands:

```
RFController(config)#wlan-qos-policy <policyname>
RFController(config)#wlan-qos-policy test
RFController(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          Configure egress prioritization multicast mask
                        (matching packets wont be queued up until DTIM)
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-WMMclients)
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
RFController(config-wlan-qos-test)#
```

## wlan-qos-policy

Table 47 Summarizes WLAN QoS Policy commands

**TABLE 47** wlan-qos-policy commands

| Command                               | Description                                                                      | Reference                |
|---------------------------------------|----------------------------------------------------------------------------------|--------------------------|
| <a href="#">accelerated-multicast</a> | Configures accelerated multicast streams address and forwards QoS classification | <a href="#">page 821</a> |
| <a href="#">classification</a>        | Classifies the traffic on the WLAN based on priority                             | <a href="#">page 822</a> |
| <a href="#">multicast-mask</a>        | Configures egress prioritization multicast mask                                  | <a href="#">page 823</a> |
| <a href="#">no</a>                    | Negates a command or sets its default values                                     | <a href="#">page 824</a> |
| <a href="#">qos</a>                   | Defines the QoS configuration                                                    | <a href="#">page 825</a> |
| <a href="#">rate-limit</a>            | Configures the traffic rate-limit on a WLAN using the WLAN QoS Policy.           | <a href="#">page 826</a> |
| <a href="#">svp-prioritization</a>    | Enables Spectralink voice protocol support on the WLAN                           | <a href="#">page 828</a> |
| <a href="#">voice-prioritization</a>  | Prioritizes voice client over other clients                                      | <a href="#">page 829</a> |
| <a href="#">wmm</a>                   | Configures 802.11e/wireless multimedia parameters                                | <a href="#">page 830</a> |

## accelerated-multicast

### *wlan-qos-policy*

Configures multicast streams for acceleration

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
accelerated-multicast [<A.B.C.D>|autodetect]
accelerated-multicast [<A.B.C.D>|autodetect] {classification}
[background|best-effort|trust|video|voice]
```

### Parameters

---

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [<A.B.C.D> autodetect]                     | • <A.B.C.D> – Configures the multicast address. It can be up to 32 IP addresses per wlan-qos-policy                                                                                                                                                                                                                                                                                                                                             |
| {classification}                           | • autodetect – Allows the system to automatically detect multicast streams                                                                                                                                                                                                                                                                                                                                                                      |
| [background best-effort trust video voice] | • classification – Configures the forwarding QoS classification (traffic class) <ul style="list-style-type: none"> <li>• background – Forwards stream with background priority</li> <li>• best-effort – Forwards stream with best-effort priority</li> <li>• trust – No change to the streams forwarding traffic class</li> <li>• video – Forwards stream with video priority</li> <li>• voice – Forwards stream with voice priority</li> </ul> |

---

### Example

```
RFController(config-wlan-qos-test)#accelerated-multicast autodetect
classification voice
RFController(config-wlan-qos-test)#
```

## classification

### *wlan-qos-policy*

Classifies traffic on the WLAN based on the priority

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
classification [low|normal|video|voice|wmm|non-unicast|non-wmm]
classification non-unicast [voice|video|normal|low|default]
classification non-wmm [voice|video|normal|low]
```

### Parameters

---

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [low normal video voice wmm non-unicast] | <ul style="list-style-type: none"> <li>• low – All the traffic on this WLAN is treated as low priority traffic (background)</li> <li>• normal – All the traffic on this WLAN is treated as normal priority (best effort)</li> <li>• video – All the traffic on this WLAN is treated as video</li> <li>• voice – All the traffic on this WLAN is treated as voice</li> <li>• wmm – Uses WMM based classification, using DSCP or 802.1p tags to classify traffic into different queues</li> <li>• non-wmm [voice video normal low] – Selects the way, the traffic from non-WMM clients must be classified</li> <li>• non-unicast [voice video normal low default] – Configures the way broadcast and multicast traffic is classified           <ul style="list-style-type: none"> <li>• voice – Non-unicast traffic is classified and treated as voice packets</li> <li>• video – Non-unicast traffic is classified and treated as video packets</li> <li>• normal – Non-unicast traffic is classified and treated as normal priority packets (best effort)</li> <li>• low – Non-unicast traffic is classified and treated as low priority packets (background)</li> <li>• default – Uses the classification mode (same as unicast classification if WMM is disabled. Normal if unicast classification is WMM)</li> </ul> </li> </ul> |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wlan-qos-test)#classification wmm
RFController(config-wlan-qos-test)#
RFController(config-wlan-qos-test)#classification normal
RFController(config-wlan-qos-test)#
RFController(config-wlan-qos-test)#classification non-unicast voice
RFController(config-wlan-qos-test)#
```



## multicast-mask

### [wlan-qos-policy](#)

Configure egress prioritization multicast mask

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
multicast-mask [primary|secondary] <WORD>
```

### Parameters

---

|                            |                                                                                                                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [primary secondary] <WORD> | Configures the primary and secondary egress prioritization multicast masks. <ul style="list-style-type: none"><li>• &lt;WORD&gt; - Specifies the MAC address and mask in AA-BB-CC-DD-EE-FF/XX-XX-XX-XX-XX-XX format</li></ul> |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-wlan-qos-test)#multicast-mask primary
11-22-33-44-55-66/22-33-44-55-66-77
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#show context
wlan-qos-policy test
  classification normal
  multicast-mask primary 11-22-33-44-55-66/22-33-44-55-66-77
  multicast-mask secondary 99-88-77-66-55-44/11-22-33-44-55-66
RFController(config-wlan-qos-test)#
```

**no***wlan-qos-policy*

Negates a command or sets its default values

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

**Syntax**

```
no [accelerated-multicast | classification | multicast-mask | qos | rate-limit |
    svp-prioritization | voice-prioritization | wmm]
```

**Parameters**


---

|                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [accelerated-multicast   classification   multicast-mask   qos   rate-limit   svp-prioritization   voice-prioritization   wmm] | <ul style="list-style-type: none"> <li>• accelerated-multicast – Disables accelerated multicast streams address and forwarding QoS classification</li> <li>• classification – Removes the classification scheme</li> <li>• multicast-mask – Clears the egress prioritization multicast mask</li> <li>• qos – Quality of service</li> <li>• rate-limit – Disables the traffic rate-limiting parameters</li> <li>• svp-prioritization – Disables support for the Spectralink voice protocol on this WLAN</li> <li>• voice-prioritization – Disables the priority of voice clients over other clients (applies to non WMM clients)</li> <li>• wmm – Disables 802.11e/wireless multimedia parameters</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

**Example**

```
RFController(config-wlan-qos-test)#no classification
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#no multicast-mask primary
RFController(config-wlan-qos-test)#
RFController(config-wlan-qos-test)#no qos trust dscp
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#show context
wlan-qos-policy test
  classification non-unicast voice
  no qos trust dscp
  qos trust wmm
  accelerated-multicast autodetect classification voice
RFController(config-wlan-qos-test)#
```

## qos

### [wlan-qos-policy](#)

Enables quality of service

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
qos trust [dscp|wmm]
```

### Parameters

---

|                  |                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| trust [dscp wmm] | Trust QOS values of ingress packets                                                                                                                             |
|                  | <ul style="list-style-type: none"><li>• dscp - Trust IP DSCP values of ingress packets</li><li>• wmm - Trust 802.11 WMM QOS values of ingress packets</li></ul> |

---

### Example

```
RFController(config-wlan-qos-test)#qos trust wmm
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#qos trust dscp
RFController(config-wlan-qos-test)#
```

## rate-limit

### wlan-qos-policy

Configures the WLAN traffic rate limit using the WLAN QoS policy

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
rate-limit [client|wlan] [from-air|to-air]
{[max-burst-size <2-102464>|rate <50-1000000>|
red-threshold [background|best-effort|video|voice]
<0-10064>]}
```

### Parameters

|                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [client wlan]                                                                                          | Configures the traffic rate-limit on a WLAN using this wlan-qos-policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| [from-air to-air]                                                                                      | <ul style="list-style-type: none"> <li>• client – Configures traffic rate limiting parameters on a per-client basis</li> <li>• wlan – Configures traffic rate limiting parameters on a per-wlan basis</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| {max-burst-size <2-1024> rate <50-1000000> red-threshold [background best-effort video voice <0-100>]} | <ul style="list-style-type: none"> <li>• from-air – Configures the traffic rate-limiting from a wireless client to the network</li> <li>• to-air – Configures the traffic rate limit from the network to a wireless client <ul style="list-style-type: none"> <li>• max-burst-size &lt;2-1024&gt; – Sets the maximum burst size from 0-1024</li> <li>• rate &lt;50-1000000&gt; – Sets the traffic rate in kbps from 50-1000000</li> <li>• red-threshold – Configures the random early detection threshold for traffic class from the list <ul style="list-style-type: none"> <li>• background &lt;0-100&gt; – Sets a threshold value for low priority traffic from 0-100</li> <li>• best-effort &lt;0-100&gt; – Sets a threshold value for normal priority traffic from 0-100</li> <li>• video &lt;0-100&gt; – Sets a threshold for video traffic from 0-100</li> <li>• voice &lt;0-100&gt; – Sets a threshold for voice traffic from 0-100</li> </ul> </li> </ul> </li> </ul> |

### Example

```
RFController(config-wlan-qos-test)#rate-limit wlan from-air max-burst-size 6
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#rate-limit wlan from-air rate 55
RFController(config-wlan-qos-test)#
```

```
RFController(config-wlan-qos-test)#rate-limit wlan from-air red-threshold
best-effort 10
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#no rate-limit wlan from-air red-threshold
best-effort
RFController(config-wlan-qos-test)#
RFController(config-wlan-qos-test)#rate-limit client from-air red-threshold
background 3
RFController(config-wlan-qos-test)#
RFController(config-wlan-qos-test)#rate-limit client from-air rate 55
RFController(config-wlan-qos-test)#
RFController(config-wlan-qos-test)#show context
wlan-qos-policy test
  voice-prioritization
  svp-prioritization
  wmm background cw-max 8
  wmm video txop-limit 9
  wmm voice cw-min 6
  wmm voice cw-max 6
  rate-limit client to-air max-burst-size 3
  rate-limit client from-air rate 55
  qos trust wmm
RFController(config-wlan-qos-test)#
```

## svp-prioritization

### [wlan-qos-policy](#)

Enables WLAN Spectralink voice protocol support

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
svp-prioritization
```

### Parameters

None

### Example

```
RFController(config-wlan-qos-test)#svp-prioritization  
RFController(config-wlan-qos-test)#
```

## voice-prioritization

### [wlan-qos-policy](#)

Prioritizes voice client over other clients (for non- WMM clients)

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
voice-prioritization
```

### Parameters

None

### Example

```
RFController(config-wlan-qos-test)#voice-prioritization  
RFController(config-wlan-qos-test)#
```

## wmm

### [wlan-qos-policy](#)

Configures 802.11e/wireless multimedia parameters

Supported in the following platforms:

- Mobility RFS7000 Controller
- Mobility RFS6000 Controller
- Mobility RFS4000 Controller
- Mobility 7131 Series Access Point
- Mobility 650 Access Point
- Mobility 6511 Access Point
- Mobility 6532 Access Point

### Syntax

```
wmm [background|best-effort|power-save|qbss-load-element|video|voice]  
wmm [background|best-effort|power-save|video|voice]  
[aifsn <2-15>|cw-max <0-15>|cw-min <0-15>|txop-limit <0-65535>]
```



## Parameters

[background|best-effort|power-save|qbss-load-element|video|voice]  
[aifsn|cw-max|cw-mintxop-limit]

- background – Configures background access category parameters
- best-effort – Configures best effort access category parameters
- video – Configures video access category parameters
- voice – Configure voice access category parameters

The following parameters are common for all the above:

- aifsn <2-15> – Configures the AIFSN: The wait time between data frames is derived from the AIFSN and slot time
  - <2-15> – Select a value between 1 and 15 to configure the AIFSN
- cw-max <0-15> – Maximum 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
  - <0-15> – ECW: the contention window. The actual value used is  $(2^{\text{ECW}} - 1)$ . Sets a value from 0-15.
- cw-min – 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
  - <0-15> – ECW: the contention window. The actual value used is  $(2^{\text{ECW}} - 1)$ . 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)
  - <0-65535> – Select a value between 0 and 65535 to configure the transmit-opportunity in 32 microsecond units
- power-save – Enables support for WMM-Powersave (U-APSD)
- qbss-load-element – Enables support for the QBSS load information element in beacons and probe responses

## Example

```
RFController(config-wlan-qos-test)#wmm background aifsn 7
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#wmm video txop-limit 9
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#wmm voice cw-min 6
RFController(config-wlan-qos-test)#

RFController(config-wlan-qos-test)#wmm qbss-load-element
RFController(config-wlan-qos-test)#
```

## NOTE

clrscr, commit, end, exit, help, revert, service, show, write are common across all chapters. For more information, see [Chapter 6, Common Commands](#).



# interface-radio Commands

---

## In this chapter

- [interface-radio Instance](#) ..... 834

Use the (config-profile-default-rfs7000) instance to configure radio instances associated with the controller.

To switch to this mode, use:

```

RFController(config-profile-default-rfs7000)#interface radio ?
  1 Radio interface 1
  2 Radio interface 2
  3 Radio interface 3
RFController(config-profile-default-rfs7000)#interface radio
RFController(config-profile-default-rfs7000-if-radio1)# ?
Radio Mode commands:
  aggregation          Configure 802.11n aggregaton related parameters
  airtime-fairness     Enable fair access to medium for clients based on
                       their usage of airtime
  antenna-gain         Specifies the antenna gain of this radio
  antenna-gain         Specifies the antenna gain of this radio
  antenna-mode         Configure the antenna mode (number of transmit and
                       receive antennas) on the radio
  beacon              Configure beacon parameters
  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
  dynamic-chain-selection Automatic antenna-mode selection (single antenna
                       for non-11n transmit rates)
  guard-interval       Configure the 802.11n guard interval
  lock-rf-mode         Retain user configured rf-mode setting for this
                       radio
  max-clients          Maximum number of wireless clients allowed to
                       associate
  mesh                Configure radio mesh parameters
  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       User short preambles on this radio
  probe-response       Configure transmission parameters for Probe
                       Response frames
  radio-tap-mode       Configure the radio-tap mode of operation for this
                       radio
  rf-mode              Configure the rf-mode of operation for this radio
  rifs                rts-threshoi
  rts-threshold        Configure the RTS threshold
  shutdown            Shutdown the selected radio interface

```

```

sniffer-redirect      Capture packets and redirect to an IP address
                      running a packet capture/analysis tool
use                   Set setting to use
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

```

```
RFController(config-profile-default-rfs7000-if-radio1)#
```

## interface-radio Instance

Table 48 Summarizes interface-radio commands

**TABLE 48** interface-radio commands

| Commands                                | Description                                                     | Reference                |
|-----------------------------------------|-----------------------------------------------------------------|--------------------------|
| <a href="#">ack-timeout</a>             | Configures the 802.11 ACK timeout                               | <a href="#">page 836</a> |
| <a href="#">aggregation</a>             | Configures 802.11n aggregations related parameters              | <a href="#">page 837</a> |
| <a href="#">airtime-fairness</a>        | Enables fair access for clients based on their usage of airtime | <a href="#">page 838</a> |
| <a href="#">antenna-diversity</a>       | Transmits antenna diversity for non-11n transmit rates          | <a href="#">page 839</a> |
| <a href="#">antenna-gain</a>            | Specifies the antenna gain of the selected radio                | <a href="#">page 840</a> |
| <a href="#">antenna-mode</a>            | Configures the antenna mode on the radio                        | <a href="#">page 841</a> |
| <a href="#">beacon</a>                  | Configures beacon parameters                                    | <a href="#">page 842</a> |
| <a href="#">channel</a>                 | Configures the channel of operation for the radio               | <a href="#">page 843</a> |
| <a href="#">data-rates</a>              | Specifies the 802.11 rates supported on the radio               | <a href="#">page 844</a> |
| <a href="#">description</a>             | Configures a description for the selected radio                 | <a href="#">page 846</a> |
| <a href="#">dynamic-chain-selection</a> | Enables automatic antenna-mode selection                        | <a href="#">page 847</a> |
| <a href="#">guard-interval</a>          | Configures the 802.11n guard interval                           | <a href="#">page 848</a> |
| <a href="#">lock-rf-mode</a>            | Retains user configured rf-mode settings for the selected radio | <a href="#">page 849</a> |

**TABLE 48** interface-radio commands

| Commands                | Description                                                                            | Reference                |
|-------------------------|----------------------------------------------------------------------------------------|--------------------------|
| <i>max-clients</i>      | Defines the maximum number of wireless clients allowed to associate                    | <a href="#">page 850</a> |
| <i>mesh</i>             | Configures radio mesh parameters                                                       | <a href="#">page 851</a> |
| <i>no</i>               | Negates a command or sets its default value                                            | <a href="#">page 852</a> |
| <i>non-unicast</i>      | Configures handling of non-unicast frames                                              | <a href="#">page 853</a> |
| <i>off-channel-scan</i> | Enables off-channel scanning on the radio                                              | <a href="#">page 854</a> |
| <i>placement</i>        | Configures the location where the radio is in operation                                | <a href="#">page 855</a> |
| <i>power</i>            | Configures the transmit power on the radio                                             | <a href="#">page 856</a> |
| <i>preamble-short</i>   | Configures user short preambles on the radio                                           | <a href="#">page 857</a> |
| <i>probe-response</i>   | Configures transmission parameters for probe response frames                           | <a href="#">page 858</a> |
| <i>radio-share-mode</i> | Configures the radio-tap mode for the radio                                            | <a href="#">page 859</a> |
| <i>rf-mode</i>          | Configures the rf-mode for the radio                                                   | <a href="#">page 860</a> |
| <i>rifs</i>             | Configures <i>Reduced Interframe Spacing</i> (RIFS) parameters                         | <a href="#">page 861</a> |
| <i>rts-threshold</i>    | Configures RTS threshold value                                                         | <a href="#">page 862</a> |
| <i>shutdown</i>         | Terminates the selected radio interface                                                | <a href="#">page 863</a> |
| <i>sniffer-redirect</i> | Captures packets and redirects to an IP address running a packet capture/analysis tool | <a href="#">page 864</a> |
| <i>use</i>              | Sets setting to use                                                                    | <a href="#">page 865</a> |
| <i>wlan</i>             | Enables WLAN on the radio                                                              | <a href="#">page 866</a> |
| <i>wireless-client</i>  | Configures wireless client related parameters                                          | <a href="#">page 868</a> |

## ack-timeout

### *interface-radio commands*

Configures the 802.11 ACK timeout

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

```
ack-timeout <1-100>
```

### **Parameters**

---

|         |                                                             |
|---------|-------------------------------------------------------------|
| <1-100> | Configures 802.11 ACK timeout between 1 to 100 microseconds |
|---------|-------------------------------------------------------------|

---

### **Example**

```
RFController(config-profile-default-rfs4000-if-radio1)#ack-timeout 10  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## aggregation

### *interface-radio commands*

Configures 802.11n aggregations related parameters

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
aggregation [ampdu|amsdu]
aggregation ampdu [rx-only|tx-only|tx-rx|none|max-aggr-size|min-spacing]
aggregation ampdu max-aggr-size[rx|tx]
aggregation ampdu max-aggr-size rx [8191|16383|32767|65535]
aggregation ampdu max-aggr-size tx [<0-65535>]
aggregation amsdu [rx-only|tx-rx]
aggregation ampdu min-spacing [0|1|2|4|8|16]]
]
```

### Parameters

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ampdu [rx-only tx-only tx-rx none max-aggr-size min-spacing] | <p>ampdu – Configures <i>Aggregate MAC Protocol Data Unit (A-MPDU)</i> parameters</p> <ul style="list-style-type: none"> <li>• tx-only – Supports transmission of AMPDU parameters only</li> <li>• rx-only – Supports receiving of AMPDU parameters only</li> <li>• tx-rx – Supports both transmit as well as receiving of AMPDU parameters</li> <li>• none – Disables support for AMPDUs</li> <li>• max-aggr-size [rx tx] – Configures limits on AMPDU packet sizes           <ul style="list-style-type: none"> <li>• rx [8191 16383 32767 65535] – Sets the limit on received frames               <ul style="list-style-type: none"> <li>• 8191 – Advertises a maximum of 8191 bytes</li> <li>• 16383 – Advertises a maximum of 16383 bytes</li> <li>• 32767 – Advertises a maximum of 32767 bytes</li> <li>• 65535 – Advertises a maximum of 65535 bytes</li> </ul> </li> <li>• tx [&lt;0-65535&gt;] – Sets the limit on transmitted frames               <ul style="list-style-type: none"> <li>• &lt;0-65535&gt; – Set the limit in bytes</li> </ul> </li> </ul> </li> <li>• min-spacing – Configures the minimum gap between AMPDU frames</li> </ul> |
| amsdu [rx-only tx-rx]                                        | <p>amsdu – Configures <i>Aggregate MAC Service Data Unit (A-MSDU)</i> parameters</p> <ul style="list-style-type: none"> <li>• rx-only – Supports receiving of A-MSDU parameters only</li> <li>• tx-rx – Supports both transmit as well as receiving of A-MSDU parameters</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#aggregation ampdu
tx-only
RFController(config-profile-default-rfs4000-if-radio1)#
```

## airtime-fairness

### *interface-radio commands*

Enables equal access for clients based on their usage of airtime

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

- 
- |                                                  |                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>{prefer-ht} {weight<br/>&lt;1-10&gt;}</pre> | <ul style="list-style-type: none"> <li>• prefer-ht – Prefers high throughput (802.11n) clients over legacy clients&gt;</li> <li>• weight &lt;1-10&gt; – Configures the relative weightage for 11n clients over legacy clients           <ul style="list-style-type: none"> <li>• &lt;1-10&gt; – Specify a weightage ratio for 11n clients between &lt;1-10&gt;</li> </ul> </li> </ul> |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
- 

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#airtime-fairness  
prefer-ht weight 1  
RFController(config-profile-default-rfs4000-if-radio1)#
```



## antenna-diversity

### *interface-radio commands*

Transmits antenna diversity for non-11n transmit rates

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

```
antenna-diversity
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default-ap7131-if-radiol)#antenna-diversity  
RFController(config-profile-default-ap7131-if-radiol)#
```

## antenna-gain

### *interface-radio commands*

Specifies the antenna gain of the selected radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|            |                                                            |
|------------|------------------------------------------------------------|
| <0.0-15.0> | Select the antenna gain in units of dBi between <0.0-15.0> |
|------------|------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#antenna-gain 1.0  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## antenna-mode

### *interface-radio commands*

Configures the antenna mode on the radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|                       |                                                                                                                                                                                                                                                                                                     |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1*1 1*3 2*2 default] | <ul style="list-style-type: none"><li>• 1x1 - Uses only antenna A to receive and transmit</li><li>• 1x3 - Uses antenna A to transmit, and receives on other antennas</li><li>• 2x2 - Uses antenna A and C for both transmit and receive</li><li>• default - Uses default antenna settings</li></ul> |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#antenna-mode 2x2
RFController(config-profile-default-rfs4000-if-radio1)#
```

## beacon

### *interface-radio commands*

Configures beacon parameters

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
beacon [dtim-period|period]
beacon dtim-period [<1-50>|bss <1-8> <1-50>]
beacon period [50|100|200]
```

### Parameters

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dtim-period         | Configures the dtim interval used on the radio <ul style="list-style-type: none"> <li>• &lt;1-50&gt; - Specify a single value used on the radio</li> <li>• bss &lt;1-8&gt; &lt;1-50&gt; - Specify a separate dtim value for bss on the radio <ul style="list-style-type: none"> <li>• &lt;1-8&gt; - Specify the bss number between &lt;1-8&gt; <ul style="list-style-type: none"> <li>• &lt;1-50&gt; - Specify the dtim value used on a selected bss</li> </ul> </li> </ul> </li> </ul> |
| period [50 100 200] | Configures the beacon interval <ul style="list-style-type: none"> <li>• 50 - 50 K-uSec interval between beacons</li> <li>• 100 - 100 K-uSec interval between beacons (default)</li> <li>• 200 - 200 K-uSec interval between beacons</li> </ul>                                                                                                                                                                                                                                          |

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#beacon dtim-period bss
2 20
RFController(config-profile-default-rfs4000-if-radio1)#

RFController(config-profile-default-rfs4000-if-radio1)#beacon period 50
RFController(config-profile-default-rfs4000-if-radio1)#

RFController(config-profile-default-rfs4000-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
 beacon dtim-period bss 4 2
 beacon dtim-period bss 5 2
 beacon dtim-period bss 6 2
 beacon dtim-period bss 7 2
 beacon dtim-period bss 8 2
 wlan wlan1 bss 1 primary
 antenna-gain 1.0
 aggregation ampdu tx-only
 antenna-mode 2x2
 airtime-fairness prefer-ht weight 1
RFController(config-profile-default-rfs4000-if-radio1)#
```

## channel

### *interface-radio commands*

Configures the channel of operation on the radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
channel [smart|12|3|4|-----]
```

### Parameters

---

|                     |                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| smart 12 3 4 -----] | <ul style="list-style-type: none"><li>• smart - Uses Smart RF to assign a channel (uses uniform spectrum spreading if Smart RF is not enabled)</li><li>• 1- Channel 1 in 20Mhz</li><li>• 2- Channel 1 in 20Mhz</li></ul> |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#channel smart  
RFController(config-profile-default-rfs4000-if-radio1)#
```

```
RFController(config-profile-default-rfs4000-if-radio1)#channel 1  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## data-rates

### *interface-radio commands*

Specifies the 802.11 rates supported on the radio

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

```
data-rates [b-only|g-only|a-only|bg|bgn|gn|an|default|custom  
data-rates custom [1|2|5.5|6|9|11|12|18|24|36|48|54| mcs0-7|mcs8-15|  
mcs0-15|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-mcs0-7]]
```

**Parameters**

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| b-only  | Supports operation in 11b-only mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| g-only  | Uses rates that support operation in 11g-only mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| a-only  | Uses rates that support operation in 11a-only mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| bg      | Uses rates that support both 11b and 11g clients                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| bgn     | Uses rates that support 11b, 11g and 11n clients                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| gn      | Uses rates that support 11g and 11n clients                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| an      | Uses rates that support 11a and 11n clients                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| default | Enables the default data-rates according to the band of operation of the radio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| custom  | <p>Configures a list of data rates by specifying each rate individually. Use 'basic-' prefix before a rate to indicate it is to be used as a basic rate (Eg: 'data-rates custom basic-1 basic-2 5.5 11')</p> <ul style="list-style-type: none"> <li>• 1 - 1-Mbps</li> <li>• 2 - 2-Mbps</li> <li>• 5.5 - 5.5-Mbps</li> <li>• 6 - 6-Mbps</li> <li>• 9 - 9-Mbps</li> <li>• 11- 11-Mbps</li> <li>• 12 - 12-Mbps</li> <li>• 18 -18-Mbps</li> <li>• 24 - 24-Mbps</li> <li>• 36 - 36-Mbps</li> <li>• 48 - 48-Mbps</li> <li>• 54 - 54-Mbps</li> <li>• mcs0-7 - Modulation and Coding Scheme 0-7</li> <li>• mcs8-15 - Modulation and Coding Scheme 8-15</li> <li>• mcs0-15 - Modulation and Coding Scheme 0-15</li> <li>• basic-1 - Basic 1-Mbps</li> <li>• basic-2 - Basic 2-Mbps</li> <li>• basic-5.5 - Basic 5.5-Mbps</li> <li>• basic-6 - Basic 6-Mbps</li> <li>• basic-9 - Basic 9-Mbps</li> <li>• basic-11 - Basic 11-Mbps</li> <li>• basic-12 - Basic 12-Mbps</li> <li>• basic-18 - Basic 18-Mbps</li> <li>• basic-24 - Basic 24-Mbps</li> <li>• basic-36 - Basic 36-Mbps</li> <li>• basic-48 - Basic 48-Mbps</li> <li>• basic-54 - Basic 54-Mbps</li> <li>• basic-mcs0-7 - Modulation and Coding Scheme 0-7 as a basic rate</li> </ul> |

**Example**

```

RFController(config-profile-default-rfs4000-if-radio1)#data-rates
b-only
RFController(config-profile-default-rfs4000-if-radio1)#
RFController(config-profile-default-rfs4000-if-radio1)#data-rates default
RFController(config-profile-default-rfs4000-if-radio1)#
RFController(config-profile-default-rfs4000-if-radio1)#data-rates custom
basic-mcs0-7
RFController(config-profile-default-rfs4000-if-radio1)#

```

## description

### *interface-radio commands*

Configures a description for the selected radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
description <WORD>
```

### Parameters

---

|        |                                                 |
|--------|-------------------------------------------------|
| <WORD> | Configures a description for the selected radio |
|--------|-------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#description radio1  
RFController(config-profile-default-rfs4000-if-radio1)#
```



## dynamic-chain-selection

### *interface-radio commands*

Enables automatic antenna-mode selection (single antenna for non-11n transmit rates)

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

```
dynamic-chain-selection
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default-rfs4000-if-radio1)#dynamic-chain-selectio  
n  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## guard-interval

### *interface-radio commands*

Configures the 802.11n guard interval

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

|      |                                                                              |
|------|------------------------------------------------------------------------------|
| any  | Allows the radio to use any short (400nSec) or long (800nSec) guard interval |
| long | Specify the use of long guard interval (800nSec)                             |

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#guard-interval long  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## lock-rf-mode

### *interface-radio* commands

Retains user configured rf-mode settings for the selected radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
lock-rf-mode
```

### Parameters

None

### Example

```
RFController(config-profile-default-rfs4000-if-radiol)#lock-rf-mode  
RFController(config-profile-default-rfs4000-if-radiol)#
```

## max-clients

### *interface-radio commands*

Defines the maximum number of wireless clients allowed to associate

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

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

### **Parameters**

---

|         |                                                                           |
|---------|---------------------------------------------------------------------------|
| <0-256> | Specify the maximum number of clients allowed to associate with the radio |
|---------|---------------------------------------------------------------------------|

---

### **Example**

```
RFController(config-profile-default-rfs4000-if-radio1)#max-clients 12  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## mesh

### *interface-radio commands*

Configures radio mesh parameters

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [client links <1-6><br> portal preferred-peer <1-6><br><MAC>] | <ul style="list-style-type: none"> <li>• client – Enables operation as a client. (Scan for mesh portals, or nodes that have connectivity to portals, and connect through them)</li> <li>• links &lt;1-6&gt; – Configures the maximum number of mesh links that the radio will attempt to create           <ul style="list-style-type: none"> <li>• &lt;1-6&gt; – Specify the maximum number of mesh links from the radio</li> </ul> </li> <li>• portal – Enables operation as a portal. (Begins beaconing immediately, accepting connections from other mesh nodes. Typically the node with a connection to the wired network)</li> <li>• preferred-peer &lt;1-6&gt; &lt;MAC&gt; – Configures a peer device to which connection should be preferred           <ul style="list-style-type: none"> <li>• &lt;1-6&gt; – Configures the priority at which the peer node will be added               <ul style="list-style-type: none"> <li>• &lt;MAC&gt; – Specify the MAC address of the preferred peer device (Ethernet MAC of either an AP or a controller with onboard radios)</li> </ul> </li> </ul> </li> </ul> |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#mesh preferred-peer 2
11-22-33-44-55-66
RFController(config-profile-default-rfs4000-if-radio1)#

RFController(config-profile-default-rfs4000-if-radio1)#mesh client
RFController(config-profile-default-rfs4000-if-radio1)#
```

## no

### *interface-radio commands*

Negates a command or sets its default value

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
no <parameter>
```

### Parameters

None

### Usage Guidelines

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

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#no aggregation ampu  
max-aggr-size rx  
RFController(config-profile-default-rfs4000-if-radio1)#
```

```
RFController(config-profile-default-rfs4000-if-radio1)#no mesh links  
RFController(config-profile-default-rfs4000-if-radio1)#
```

```
RFController(config-profile-default-rfs4000-if-radio1)#no rifs mode  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## non-unicast

### *interface-radio* commands

Configures handling of non-unicast frames

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
non-unicast [forwarding|queue|tx-rate]
non-unicast forwarding [follow-dtim|power-save-aware]
non-unicast queue [<1-200>|bss <1-8> <1-200>]
non-unicast tx-rate [bss
<1-8>|dynamic-all|dynamic-basic|highest-basic|lowest-basic]
non-unicast tx-rate bss <1-8> {dynamic-all|dynamic-basic|highest-basic|
lowest-basic}
```

### Parameters

|                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| forwarding [follow-dtim   power-save-aware]                                      | Configures the method by which multicast and broadcast frames are forwarded by the radio <ul style="list-style-type: none"> <li>• follow-dtim – Specifies the frames always wait for the DTIM interval</li> <li>• power-save-aware – If all associated wireless-clients are in a power-save active mode, then the frames are forwarded immediately</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |
| queue [<1-200> bss <1-8> <1-200>]                                                | Configures the number of broadcast packets that are queued up per bss on the radio <ul style="list-style-type: none"> <li>• &lt;1-200&gt; – Specify the number of packets per bss</li> <li>• bss &lt;1-8&gt; &lt;1-200&gt; – Overrides the default on a specific bss number <ul style="list-style-type: none"> <li>• &lt;1-8&gt; &lt;1-200&gt; – Specify the bss number</li> <li>• &lt;1-200&gt; – Specifies the number of packets queued</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                             |
| tx-rate [bss <1-8>   dynamic-all   dynamic-basic   highest-basic   lowest-basic] | Configures the data-rate at which broadcast and multicast frames will be transmitted <ul style="list-style-type: none"> <li>• bss &lt;1-8&gt; {dynamic-all   dynamic-basic   highest-basic   lowest-basic} – Overrides the default on a specific bss number <ul style="list-style-type: none"> <li>• &lt;1-8&gt; – Specify the bss number</li> </ul> </li> <li>• dynamic-all – Select a rate among all the supported rates based on current traffic conditions</li> <li>• dynamic-basic – Select a rate among all the basic rates based on current traffic conditions</li> <li>• highest-basic – Uses the highest configured basic rate on the radio</li> <li>• lowest-basic – Uses the lowest configured basic rate on the radio</li> </ul> |

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#non-unicast queue bss
2 3
RFController(config-profile-default-rfs4000-if-radio1)#
RFController(config-profile-default-rfs4000-if-radio1)#non-unicast tx-rate
bss 1 dynamic-all
RFController(config-profile-default-rfs4000-if-radio1)#
```

## off-channel-scan

### *interface-radio commands*

Enables off-channel scanning on the radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
off-channel-scan {channel-list [2.4Ghz {<WORD>}|5Ghz
{<WORD>}]|sniffer-redirect <A.B.C.D>}
```

### Parameters

|                                              |                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| channel-list [2.4Ghz {<WORD>} 5Ghz {<WORD>}] | channel-list [2.4GHz {<WORD>} 5GHz {<WORD>} - Specifies the channel list to scan <ul style="list-style-type: none"> <li>• 2.4GHz &lt;WORD&gt; - 2.4GHz band</li> <li>• 5GHz &lt;WORD&gt; - 5GHz band <ul style="list-style-type: none"> <li>• &lt;WORD&gt; - Specify a list of 20MHz/40MHz channels</li> </ul> </li> </ul> |
| sniffer-redirect <A.B.C.D>                   | Captures packets and redirects to an IP address running a packet capture analysis tool <ul style="list-style-type: none"> <li>• &lt;A.B.C.D&gt; - Specify the IP address of the destination device</li> </ul>                                                                                                              |

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#off-channel-scan
channel-list 2.4GHz 1
RFController(config-profile-default-rfs4000-if-radio1)#

RFController(config-profile-default-rfs4000-if-radio1)#off-channel-scan
channel-list 5GHz
RFController(config-profile-default-rfs4000-if-radio1)#
```



## placement

### *interface-radio commands*

Configures the location where the radio is in operation

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|                  |                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [indoor outdoor] | <ul style="list-style-type: none"><li>• indoor – Radio is deployed indoors (uses indoor regulatory rules)</li><li>• outdoor – Radio is deployed outdoors (uses outdoor regulatory rules)</li></ul> |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#placement outdoor
RFController(config-profile-default-rfs4000-if-radio1)#
```

## power

### *interface-radio commands*

Configures the transmit power on the radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
power [<1-27>|smart]
```

### Parameters

---

|              |                                                                                                                                                                                                                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-27> smart | <ul style="list-style-type: none"><li>• &lt;1-27&gt; - Transmits power in dBm (actual power could be lower based on regulatory restrictions)</li><li>• smart - Smart RF decides optimum power required</li></ul> |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#power smart  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## preamble-short

### *interface-radio commands*

Configures short preamble on the radio

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

```
preamble-short
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default-rfs4000-if-radiol)#preamble-short  
RFController(config-profile-default-rfs4000-if-radiol)#
```

## probe-response

### *interface-radio commands*

Configures transmission parameters for probe response frames

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rate [follow-probe-request highest-basic lowest-basic] | Configures the data rates at which the probe responses are transmitted <ul style="list-style-type: none"> <li>• follow-probe-request – Transmits probe responses at the same rate the request was received</li> <li>• highest-basic – Uses the highest configured basic rate of the radio</li> <li>• lowest-basic – Uses the lowest configured basic rate of the radio</li> </ul> |
| retry                                                  | Retransmits probe response if no acknowledgement is received from the client                                                                                                                                                                                                                                                                                                      |

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#probe-response retry
RFController(config-profile-default-rfs4000-if-radio1)#

RFController(config-profile-default-rfs4000-if-radio1)#probe-response rate
highest-basic
RFController(config-profile-default-rfs4000-if-radio1)#
```

## radio-share-mode

### *interface-radio commands*

Configures the radio-share mode of operation for this radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [inline off promiscuous] | <ul style="list-style-type: none"><li>• inline – Enables sharing of all wlan packets serviced by this radio (matching the bssid of the radio)</li><li>• off – Disables radio-share (no packets shared with wips sensor module)</li><li>• promiscuous – Enables sharing of all packets that the radio can receive in promiscuous mode without filtering based on its bssid</li></ul> |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-ap7131-if-radio1)#radio-share-mode  
promiscuous  
RFController(config-profile-default-ap7131-if-radio1)#
```

```
RFController(config-profile-default-ap7131-if-radio1)#radio-share-mode inline  
RFController(config-profile-default-ap7131-if-radio1)#
```

## rf-mode

### *interface-radio commands*

Configures the rf-mode for the radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
rf-mode [2.4GHz-wlan|5GHz-wlan|sensor]
```

### Parameters

---

|                     |                                                                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.4GHz 5GHz sensor] | <ul style="list-style-type: none"><li>• 2.4GHz-wlan - Provides WLAN service in 2.4GHz band</li><li>• 5GHz-wlan - Provides WLAN service in 5GHz band</li><li>• sensor - Operates as a sensor radio</li></ul> |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#rf-mode sensor  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## rifs

### *interface-radio commands*

Configures *Reduced Interframe Spacing* (RIFS) parameters

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|                              |                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [none rx-only tx-only tx-rx] | <ul style="list-style-type: none"><li>• none - Disables support for RIFS</li><li>• rx-only - Supports RIFS possession only</li><li>• tx-only - Support RIFS transmission only</li><li>• tx-rx- Supports both RIFS transmission and possession</li></ul> |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#rifs tx-rx  
RFController(config-profile-default-rfs4000-if-radio1)#
```

```
RFController(config-profile-default-rfs4000-if-radio1)#rifs tx-only  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## rts-threshold

### *interface-radio commands*

Configures RTS threshold value

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
rts-threshold <0-2347>
```

### Parameters

---

|          |                                                 |
|----------|-------------------------------------------------|
| <0-2347> | Specify RTS threshold in bytes between <0-2347> |
|----------|-------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#rts-threshold 10  
RFController(config-profile-default-rfs4000-if-radio1)#
```



## shutdown

### *interface-radio commands*

Terminates the selected radio interface

Supported in the following platforms:

- Mobility RFS4011

### **Syntax**

```
shutdown
```

### **Parameters**

None

### **Example**

```
RFController(config-profile-default-rfs4000-if-radiol)#shutdown  
RFController(config-profile-default-rfs4000-if-radiol)#
```

## sniffer-redirect

### *interface-radio commands*

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

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
sniffer-redirect <A.B.C.D> channel [1|1+|10|10-----165
```

### Parameters

---

|                      |                                                                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <A.B.C.D> channel    | <A.B.C.D> - Specify the IP address of the destination device                                                                                                                                                                                                                                                    |
| [1 1+ 10 10-----165] | <ul style="list-style-type: none"> <li>• channel [1 1+ 10 10-----165 - Specify the channel to capture packets           <ul style="list-style-type: none"> <li>• 1 - Channel 1 in 20Mhz</li> <li>• 1+ - Channel 1 as primary, Channel 5 as extension</li> <li>• 10 - Channel 10 in 20Mhz</li> </ul> </li> </ul> |

---

### Example

```
RFController(config-profile-default-rfs4000-if-radiol)#sniffer-redirect
172.16.10.13 channel ?
  1      Channel 1 in 20Mhz
  1+     Channel 1 as primary, Channel 5 as extension
  10     Channel 10 in 20Mhz
  10-    Channel 10 as primary, Channel 6 as extension
  100    Channel 100 in 20Mhz
-----
RFController(config-profile-default-rfs4000-if-radiol)#
```

## USE

### *interface-radio commands*

Sets setting to use

Supported in the following platforms:

- Mobility RFS4011

## Syntax

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

## Parameters

---

|                                                                   |                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [association-acl-policy <ASSOC-ACL> radio-qos-policy <RADIO-QOS>] | <ul style="list-style-type: none"><li>• [association-acl-policy &lt;ASSOC-ACL&gt; - Specify the name of the association-acl-policy used</li><li>• radio-qos-policy &lt;RADIO-QOS&gt; - Specify the name of the radio-qos-policy used</li></ul> |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Example

```
RFController(config-profile-default-rfs4000-if-radio1)#use  
association-acl-policy test  
RFController(config-profile-default-rfs4000-if-radio1)#
```

## wlan

### *interface-radio commands*

Enables WLAN on the radio

Supported in the following platforms:

- Mobility RFS4011

### Syntax

```
wlan <WLAN> {bss|primary}
wlan <WLAN> bss <1-8> {primary}
```

### Parameters

---

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;WLAN&gt; {bss &lt;1-8&gt;  primary}</code> | <p><code>&lt;WLAN&gt; {bss &lt;1-8&gt;  primary}</code> – Specify the name of the WLAN (it must have been already created and configured)</p> <ul style="list-style-type: none"> <li>• <code>bss &lt;1-8&gt; {primary}</code> – Optional. Provide a specific bss number on the radio where the selected WLAN has to be mapped           <ul style="list-style-type: none"> <li>• <code>&lt;1-8&gt;</code> – Specify the bss number</li> </ul> </li> <li>• <code>primary</code> – Optional. Pretends the selected WLAN as the primary WLAN if there are multiple WLANs on its bss</li> </ul> |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#wlan wlan1
RFController(config-profile-default-rfs4000-if-radio1)#

RFController(config-profile-default-rfs4000-if-radio1)#show context
interface radiol
  rf-mode sensor
  placement outdoor
  beacon dtim-period bss 1 2
  beacon dtim-period bss 2 3
  beacon dtim-period bss 3 2
  beacon dtim-period bss 4 2
  beacon dtim-period bss 5 2
  beacon dtim-period bss 6 2
  beacon dtim-period bss 7 2
  beacon dtim-period bss 8 2
  rts-threshold 10
  wlan wlan1 bss 1 primary
  off-channel-scan channel-list 5GHz
  off-channel-scan channel-list 2.4GHz 1
  off-channel-scan sniffer-redirect 172.16.10.100
  rifs tx-rx
  use association-acl-policy test
  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 queue bss 1 2
  non-unicast queue bss 2 1
  non-unicast queue bss 3 1
```

```
non-unicast queue bss 4 1
non-unicast queue bss 5 1
non-unicast queue bss 6 1
non-unicast queue bss 7 1
non-unicast queue bss 8 1
probe-response rate highest-basic
RFController(config-profile-default-rfs4000-if-radiol)#
```

## wireless-client

### *interface-radio commands*

Configures wireless client related parameters

Supported in the following platforms:

- Mobility RFS4011

### Syntax

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

### Parameters

---

|                 |                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------|
| tx-power <0-20> | Configures the transmit power indicated to wireless clients                                                  |
|                 | <ul style="list-style-type: none"><li>• &lt;0-20&gt; – Specify transmit power between 0 and 20 dBm</li></ul> |

---

### Example

```
RFController(config-profile-default-rfs4000-if-radio1)#wireless-client  
tx-power 2  
RFController(config-profile-default-rfs4000-if-radio1)#
```

# Firewall Logging

---

## In this chapter

- [Firewall Log Terminology and Syslog Severity Levels . . . . .](#) 869

This chapter summarizes the Firewall Logging commands within the CLI.

The firewall uses logging to send system messages to one or more logging destinations, where they can be collected, archived and reviewed.

Set the logging level to define which messages are sent to each of the target destinations.

Logging messages can be sent to any of the following destinations:

- The firewall console
- Telnet or SSH sessions to the firewall
- A temporary buffer internal to the firewall
- Syslog servers
- E-mail addresses
- An FTP server

## Firewall Log Terminology and Syslog Severity Levels

| Abbreviation           | Description                                                                                   |
|------------------------|-----------------------------------------------------------------------------------------------|
| FTP                    | File transfer protocol                                                                        |
| ACL                    | Access control list                                                                           |
| Src MAC                | Source MAC address                                                                            |
| Dest MAC               | Destination MAC address                                                                       |
| LOGRULEHIT             | ACL rule applied                                                                              |
| PKT DROP               | Packet drop                                                                                   |
| Src IP                 | Source IP address                                                                             |
| Dest IP / Dst IP       | Destination IP address                                                                        |
| FWSTARTUP              | Firewall enabled                                                                              |
| DP                     | Destination port                                                                              |
| SP                     | Source port                                                                                   |
| Matched Temporary Rule | This is a internal rule created to allow data traffic for ALG like TFTP, FTP, HTTPs and so on |

| Syslog Severity Level as Message | Severity Level as Numeric | Description                      |
|----------------------------------|---------------------------|----------------------------------|
| emergency                        | 0                         | System is unusable               |
| alert                            | 1                         | Immediate action needed          |
| critical                         | 2                         | Critical condition               |
| error                            | 3                         | Error condition                  |
| warning                          | 4                         | Warning condition                |
| notification                     | 5                         | Normal but significant condition |
| informational                    | 6                         | Informational message            |
| debugging                        | 7                         | Debugging message                |

## Date format in Syslog messages

The following output displays date in proper format

```
rfs7000-81916A(config)#May 19 16:20:00 2010: USER: cfgd: deleting session 4
rfs7000-81916A(config)#
rfs7000-81916A(config)#May 19 16:20:17 2010: USER: cfgd: deleting session 5
The date format is Month<MMM> Date <DD> Time <HH:MM:SS> Year <YYYY>
Month is May
Date is 19
Time is 16:20:00
Year is 2010
To generate a date log, enable logging
```

For example, the following command has to be executed.

```
RFController#clock set 16:20:00 19 May 2010
RFController#
```

## FTP data connection log

To generate a FTP data connection log, an ACL rule has to be applied, and logging has to be enabled.

### *The FTP connection is Control Connection*

```
May 19 16:31:19 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.2.102 Proto:6 Src Port:3014 Dst Port:21
Date is May19
Time is 16:31:19
Year is 2010
Module name is DATAPLANE
Syslog Severity level is 5
Log ID is LOGRULEHIT
Log Message is Matched ACL
The Matching ACL is FTPuser
ip Rule sequence number is 0
```



```
Disposition is Allow Packet
Source MAC Address is 00-19-B9-6B-DA-77
Destination MAC Address is <00-15-70-81-91-6A>
Ethertype is 0x0800
Source IP Address is 192.168.1.99
Destination IP Address is 192.168.2.102
Protocol Type is 6
Source Port is 3014D
Destination Port is 21
```

**NOTE**

The same terminology is used across all logs.

***The Data Connection in Active Mode***

```
May 19 16:35:54 2010: %DATAPLANE-5-LOGRULEHIT: Matched Temporary Rule of FTP
ALG. Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:192.168.1.99 Proto:6 Src Port:20 Dst Port:3017.
```

***The Data Connection in Passive Mode***

```
May 19 17:14:31 2010: %DATAPLANE-5-LOGRULEHIT: Matched Temporary Rule of FTP
ALG. Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.2.102 Proto:6 Src Port:3033 Dst Port:3894.
```

For example,

```
RFController(config-mac-acl-test)#permit any any log rule-precedence 25
RFController(config-mac-acl-test)#
```

**UDP packets log**

In both DHCP release and DHCP renew scenarios, the destination port 67 is logged.

***DHCP Release***

```
May 19 18:57:43 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1
Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:172.16.31.196 Proto:17 Src Port:68 Dst Port:67.
```

***DHCP Renew***

```
May 19 18:58:48 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1
Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<FF-FF-FF-FF-FF-FF> Ethertype:0x0800 Src IP:0.0.0.0 Dst IP:255.255.255.255
Proto:17 Src Port:68 Dst Port:67.
```

To generate a UDP packet log, an ACL rule has to be applied to UDP packets and logging has to be enabled.

For example,

```
RFController(config-ip-acl-test)#permit udp any any log rule-precedence 20
RFController(config-ip-acl-test)#
```

## ICMP type logs

The example below displays an ICMP Type as 13 and an ICMP Code as 0.

```
May 19 19:12:13 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:192.168.1.103 Proto:1 ICMP Type:13 ICMP Code:0.
```

The below example displays an ICMP Type as 15 and an ICMP Code as 0.

```
May 20 10:35:49 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Allow Packet Src MAC:<00-60-80-B0-C3-E3> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.104 Dst
IP:192.168.2.102 Proto:1 ICMP Type:15 ICMP Code:0.
```

The below example displays an ICMP Type as 17 and an ICMP Code as 0.

```
May 19 19:26:18 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:192.168.1.103 Proto:1 ICMP Type:17 ICMP Code:0.
```

The below example displays an ICMP Type as 18 and an ICMP Code as 0.

```
May 20 10:28:24 2010: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP
type 18. Reason: no flow matching payload of ICMP Reply.
Module name is DATAPLANE
Syslog Severity level is 5
Log ID is ICMPPKTDROP
Log Message is Dropping ICMP Packet
```

To generate an ICMP log, an ACL rule has to be applied on ICMP packets, and logging has to be enabled.

For example, the following commands have to be executed.

```
RFController(config-ip-acl-test)#permit icmp any any log rule-precedence 20
RFController(config-ip-acl-test)#
```

## ICMP type logs

The following example displays an ICMP Type as 3 and a Code as 3.

```
May 19 19:56:00 2010: %DATAPLANE-5-ICMPPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP
type 3. Reason: no flow matching payload of ICMP Error.
Module name is DATAPLANE
Syslog Severity level is 5
Log ID is ICMPPKTDROP
Log Message is Dropping ICMP Packet
```

The following example displays an ICMP Type as 4 and a Code as 0.

```
May 19 21:13:36 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP
type 4. Reason: ICMP dest IP does not match inner source IP.
```

The following example displays an ICMP Type as 5 and a Code as 0.

```
May 19 21:15:12 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP
type 5. Reason: ICMP dest IP does not match inner source IP.
```

The following example displays an ICMP type as 11 and a Code as 0.

```
May 20 10:24:52 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.2.102 to 192.168.1.103, with ProtocolNumber:1 ICMP code 0 and ICMP
type 11. Reason: ICMP dest IP does not match inner source IP.
```

The following example displays an ICMP type as 14 and a Code as 0.

```
May 20 10:33:57 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP
type 14. Reason: no flow matching payload of ICMP Reply.
```

The following example displays an ICMP type as 16 and a Code as 0.

```
May 20 10:37:11 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 0 and ICMP
type 16. Reason: no flow matching payload of ICMP Reply.
```

To generate an ICMP log, logging has to be enabled.

For example, the following commands has to be executed.

```
RFController(config-fw-policy-default)#logging icmp-packet-drop all
RFController(config-fw-policy-default)#
```

## Raw IP Protocol logs

The following example displays a TCP header length as less than 20 bytes:

```
May 19 20:02:50 2010: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header
length less than 20 bytes : Src IP : 192.168.2.102, Dst IP: 192.168.1.104, Src
Mac: 00-11-25-14-D9-E2, Dst Mac: 00-15-70-81-91-6A, Proto = 6..
Module name is DATAPLANE
Syslog Severity level is 4
Log ID is DOSATTACK
Log Message is INVALID PACKET
May 19 20:02:50 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from
192.168.2.102 to 192.168.1.104 Protocol Number: 6. Reason: malformed TCP
header.
Module name is DATAPLANE
Syslog Severity level is 5
Log ID is MALFORMEDIP
Log Message is Dropping IPv4Packet
To generate a raw IP protocol log, logging has to be enabled.
```

For example, the following commands has to be executed.

```
RFController(config-fw-policy-default)# logging verbose
RFController(config-fw-policy-default)#
RFController(config-fw-policy-default)# logging malformed-packet-drop all
RFController(config-fw-policy-default)#
```

When logging verbose is enabled, the log is displayed as:

```
Aug 18 15:57:21 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from
192.168.0.91 to 192.168.0.1 Protocol Number: 6 SrcPort: 22616 DstPort: 22616
Reason: no matching TCP flow.
Module name is DATAPLANE
Syslog Severity level is 5
Log ID is MALFORMEDIP
Log Message is Dropping IPv4Packet
```

## Raw IP Protocol logs

The following example displays TCP without data:

```
May 19 20:02:50 2010: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header
length less than 20 bytes : Src IP : 192.168.2.102, Dst IP: 192.168.1.104, Src
Mac: 00-11-25-14-D9-E2, Dst Mac: 00-15-70-81-91-6A, Proto = 6.
May 19 20:02:50 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from
192.168.2.102 to 192.168.1.104 Protocol Number: 6. Reason: malformed TCP
header.
To generate a raw ip protocol log, logging has to be enabled.
```

For example, the following commands has to be executed.

```
RFController(config-fw-policy-default)# logging verbose
RFController(config-fw-policy-default)#
RFController(config-fw-policy-default)# logging rawip-packet-drop all
RFController(config-fw-policy-default)#
```

When logging verbose is enabled, the log is displayed as:

```
Aug 18 15:57:49 2010: %DATAPLANE-4-DOSATTACK: INVALID PACKET: TCP header
length less than 20 bytes : Src IP : 192.168.0.91, Dst IP: 192.168.0.1, Src
Mac: 00-16-36-05-72-2A, Dst Mac: 00-23-68-22-C8-6E, Proto = 6.
Aug 18 15:57:49 2010: %DATAPLANE-5-MALFORMEDIP: Dropping IPv4 Packet from
192.168.0.91 to 192.168.0.1 Protocol Number: 6 . Reason: malformed TCP header.
Module name is DATAPLANE
Syslog Severity level is 4
Log ID is DOSATTACK
Log Message is INVALID PACKET
```

## Firewall startup log

The following example displays an enabled firewall. A firewall enabled message is displayed in **bold**.

```
System bootup time (via /proc/uptime) was 93.42 42.52
Please press Enter to activate this console. May 19 20:10:09 2010:
%NSM-4-IFUP: Interface vlan2 is up
May 19 20:10:09 2010: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to
master interface.
May 19 20:10:09 2010: %NSM-4-IFUP: Interface vlan172 is up
May 19 20:10:09 2010: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to
master interface.
May 19 20:10:09 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/lighttpd"
May 19 20:10:09 2010: %FILEMGMT-5-HTTPSTART: lighttpd started in external mode
with pid 0
May 19 20:10:09 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1
May 19 20:10:09 2010: %USER-5-NOTICE: FILEMGMT[1086]: FTP: ftp server stopped
```

```

May 19 20:10:09 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1
May 19 20:10:10 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1
May 19 20:10:10 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2
May 19 20:10:10 2010: %DOT11-5-COUNTRY_CODE: Country of operation configured
to in [India]
May 19 20:10:10 2010: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from
module DOT11
May 19 20:10:10 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/telnetd"
May 19 20:10:10 2010: %AUTH-6-INFO: sshd[1422]: Server listening on 0.0.0.0
port 22.
dataplane enabled
CCB:21:Firewall enabled
May 19 20:10:11 2010: %KERN-4-WARNING: dataplane enabled.
May 19 20:10:11 2010: %DATAPLANE-5-FWSTARTUP: Firewall enabled.
May 19 20:10:13 2010: USER: cfgd: handle_cluster_member_update
May 19 20:10:13 2010: USER: cfgd: ignoring, no cluster configured
May 19 20:10:13 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"

```

## Manual time change log

The following example displays the manual time changes log. The clock is manually set to May 19 18:49:07 2010.

```

Log change in time
rfs7000-81916A#show clock
May 19 14:39:11 UTC 2010
rfs7000-81916A#clock set 18:49:00 19 May 2010
May 19 14:39:18 2010: %[S1]CFGD-6-SYSTEM_CLOCK_RESET: System clock reset,
Time: 2010-05-19 18:49:00[S2]
rfs7000-81916A#show clock
May 19 18:49:07 UTC 2010
rfs7000-81916A#

```

To generate a time log, logging has to be enabled

For example, the following command has to be executed:

```

RFController#clock set 18:49:07 19 May 2010
RFController#

```

## Firewall ruleset log

The following example displays the log changes as "ACL\_ATTACHED ALTERED" when an ACL Rule is applied/removed on WLAN, VLAN, GE, and PORT-CHANNEL.

### *IPACL IN on WLAN Attach*

```

May 21 12:48:40 2010: %CFGD-6-ACL_ATTACHED ALTERED: USER: root session 3: ACL
attached to wlan ICASA-testing is getting altered
USER: The user who is doing the change
session: means the session id of the user - one user can have multiple
sessions running, so this explains from which session this change was done
ACL : Name of the ACL that has rules added/deleted

```

***IP ACL IN on WLAN Remove***

May 21 12:49:26 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***IP ACL OUT on WLAN Attach***

May 21 12:52:49 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***IP ACL OUT on WLAN Remove***

May 21 12:52:58 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***MAC ACL IN on WLAN Attach***

May 21 12:54:25 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***MAC ACL IN on WLAN Remove***

May 21 12:54:32 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***MAC ACL OUT on WLAN Attach***

May 21 12:56:29 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***MAC ACL OUT on WLAN Remove***

May 21 12:56:37 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to wlan ICSA-testing is getting altered.

***IP ACL on VLAN Attach***

May 21 12:58:44 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

***IP ACL on VLAN Remove***

May 21 12:59:30 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to interface vlan1 is getting altered.

***IP ACL on GE Port Attach***

May 21 13:01:41 2010: %CFGD-6-ACL\_ATTACHED\_ALTERED: USER: root session 3: ACL attached to interface ge1 is getting altered.

***IP ACL on GE Port Remove***

```
May 21 13:01:25 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface gel is getting altered.
```

***MAC ACL on GE Port Attach***

```
May 21 13:03:15 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface gel is getting altered.
```

***MAC ACL on GE Port Remove***

```
May 21 13:06:19 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface gel is getting altered.
```

***IP ACL on Port-Channel Attach***

```
May 21 13:07:12 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface port-channell is getting altered.
```

***IP ACL on Port-Channel Remove***

```
May 21 13:07:26 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface port-channell is getting altered.
```

***MAC ACL on Port-Channel Attach***

```
May 21 13:09:13 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface port-channell is getting altered.
```

***MAC ACL on Port-Channel Remove***

```
May 21 13:09:24 2010: %CFGD-6-ACL_ATTACHED_ALTERED: USER: root session 3: ACL
attached to interface port-channell is getting altered.
```

***Rule added / deleted from IP/MAC ACL***

```
Feb 26 20:32:56 2010: %CFGD-6-ACL_RULE_ALTERED: USER: admin session 3: ACL foo
rule is getting altered.
```

**TCP Reset Packets log**

For any change in the TCP configuration, a TCP reset log is generated. The following example displays the initial TCP packets permitted before the session timedout.

```
May 19 20:31:26 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1
Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.2.102 Proto:6 Src Port:3318 Dst Port:21.
May 19 20:31:31 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:1
Disposition:Allow Packet Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.2.102 Proto:6 Src Port:3318 Dst Port:21.
```

## ICMP Destination log

The following example displays an ICMP destination is unreachable when no matching payload is found.

```
May 19 19:57:09 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP
type 3. Reason: no flow matching payload of ICMP Error.
May 19 19:57:09 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.1.104 to 192.168.2.102, with ProtocolNumber:1 ICMP code 3 and ICMP
type 3. Reason: no flow matching payload of ICMP Error.
```

To generate an ICMP protocol log, an ACL rule has to be applied and logging has to be enabled.

For example, the following commands has to be executed.

```
RFController(config-ip-acl-test)#permit icmp any any log rule-precedence 20
RFController(config-ip-acl-test)#
```

## ICMP Packet log

```
May 19 20:37:04 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftuser:ip Rule:0
Disposition:Drop Packet Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.1.1 Proto:1 ICMP Type:8 ICMP Code:0.
May 19 20:37:08 2010: %DATAPLANE-5-ICMPKTDROP: Dropping ICMP Packet from
192.168.2.1 to 172.16.31.196, with Protocol Number:1 ICMP code 3 and ICMP type
3. Reason: no flow matching payload of ICMP Error.
```

To generate an ICMP protocol log, an ACL rule has to be applied and logging has to be enabled.

For example, the following commands has to be executed.

```
RFController(config-ip-acl-test)#permit icmp any any log rule-precedence 20
RFController(config-ip-acl-test)#
```

## SSH connection log

A SSH connection is enabled on the controller using factory settings.

```
Running primary software, version 5.0.0.0-81243X
Alternate software Secondary, version 5.0.0.0-070D
Software fallback feature is enabled
System bootup time (via /proc/uptime) was 126.10 92.38
Please press Enter to activate this console. May 19 20:47:33 2010:
%DOT11-5-COUNTRY_CODE: Country of operation configured to in [India]
May 19 20:47:34 2010: %DIAG-6-NEW_LED_STATE: LED state message AP_LEDS_ON from
module DOT11
May 19 20:47:34 2010: KERN: vlan1: add 01:00:5e:00:00:01 mcast address to
master interface.
May 19 20:47:34 2010: %NSM-4-IFUP: Interface vlan2 is up
May 19 20:47:34 2010: KERN: vlan2: add 01:00:5e:00:00:01 mcast address to
master interface.
May 19 20:47:34 2010: %NSM-4-IFUP: Interface vlan172 is up
May 19 20:47:34 2010: KERN: vlan172: add 01:00:5e:00:00:01 mcast address to
master interface.
May 19 20:47:34 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan1
May 19 20:47:34 2010: %PM-6-PROCSTART: Starting process "/usr/sbin/sshd"
May 19 20:47:34 2010: %DAEMON-3-ERR: dhcrelay: idataplane enabled
```



```

interface allocatCCB:21:Firewall enabled
e : vlan1
May 19 20:47:34 2010: %DAEMON-3-ERR: dhcrelay: interface allocate : vlan2
May 19 20:47:34 2010: %KERN-4-WARNING: dataplane enabled.
May 19 20:47:34 2010: %DATAPLANE-5-FWSTARTUP: Firewall enabled.
May 19 20:47:39 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Drop Packet Src MAC:<00-19-B9-6B-DA-77> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.1.99 Dst
IP:192.168.1.1 Proto:6 Src Port:3327 DstPort:22.

```

## Allowed/Dropped Packets Log

The following example displays disposition information regarding allow/deny packets.

### *Allow Packets*

```

CCB:0:Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src
MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src
IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137
CCB:0:Matched ACL:ftpuser:ip Rule:1 Disposition:Allow Packet Src
MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src
IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:1029 Dst Port:53
CCB:May 19 18:14:3220100: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip
Rule:1 Disposition:Allow Packet Src MAC: 00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137.
ser:ip Rule:1 Disposition:Allow Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:192.168.2.1 Proto:17 Src Port:1029 Dst Port:53

```

### *Drop/Deny Packets*

```

CCB:0:Matched ACL:ftpuser:ip Rule:0 Disposition:Drop Packet Src
MAC:<00-11-25-14-D9-E2> Dst MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src
IP:192.168.2.102 Dst IP:192.168.2.1 Proto:17 Src Port:137 Dst Port:137
May 19 20:41:28 2010: %DATAPLANE-5-LOGRULEHIT: Matched ACL:ftpuser:ip Rule:0
Disposition:Drop Packet Src MAC:<00-11-25-14-D9-E2> Dst
MAC:<00-15-70-81-91-6A> Ethertype:0x0800 Src IP:192.168.2.102 Dst
IP:192.168.2.1 Proto:17 Src Port:137 Dst

```

To generate an allow/deny protocol log, ACL rule has to be applied and logging has to be enabled.

For example, the following commands has to be executed:

```

RFController(config-ip-acl-test)#permit ip any any log rule-precedence 20
RFController(config-ip-acl-test)#
RFController(config-ip-acl-test)#deny ip any any log rule-precedence 20
RFController(config-ip-acl-test)#

```

## 26 Firewall Log Terminology and Syslog Severity Levels

