ADTRAN OPERATING SYSTEM (AOS)

Command Reference Guide

AOS Version 11.1

NetVanta 5000 Series Products

November 2005
61200990L1-35E

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, service marks, or trade names of their respective holders.

To the Holder of this Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

Software Licensing Agreement

Each ADTRAN product contains a single license for ADTRAN supplied software. Pursuant to the Licensing Agreement, you may: (a) use the software on the purchased ADTRAN device only and (b) keep a copy of the software for backup purposes. This Agreement covers all software installed on the system as well as any software available on the ADTRAN website. In addition, certain ADTRAN systems may contain additional conditions for obtaining software upgrades.

Conventions

NOTE *Notes provide additional useful information.*

CAUTION *Cautions signify information that could prevent service interruption or damage to the equipment.*

WARNING *Warnings provide information that could prevent endangerment to human life.*

ADTRAN

901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000
www.adtran.com

Warranty and Customer Service

ADTRAN will repair and return this product within the warranty period if it does not meet its published specifications or fails while in service. Warranty information can be found at www.adtran.com. (Click on *Warranty and Repair Information* under *Support*.)

Product Registration

Registering your product helps ensure complete customer satisfaction. Please take time to register your products on line at www.adtran.com. Click *Service/Support* and then on *Product Registration* under *Support.*

Product Support Information

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

Repair and Return

If you determine that a repair is needed, please contact our Customer and Product Service (CaPS) department to have an RMA number issued. CaPS should also be contacted to obtain information regarding equipment currently in house or possible fees associated with repair.

CaPS Department	(256) 963-8722

Identify the RMA number clearly on the package (below the address), and return to the following address:

ADTRAN Customer and Product Service
901 Explorer Blvd. (East Tower)
Huntsville, Alabama 35806

RMA # _____________

Pre-Sales Inquiries and Applications Support

Your reseller should serve as the first point of contact for support. If additional pre-sales support is needed, the ADTRAN Support website provides a variety of support services such as a searchable knowledge base, latest product documentation, application briefs, case studies, and a link to submit a question to an Applications Engineer. All of this, and more, is available at:

http://support.adtran.com

When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

Applications Engineering	(800) 615-1176

Post-Sales Support

Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support website provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and trouble-shooting tools. All of this, and more, is available at:

http://support.adtran.com

When needed, further post-sales assistance is available by calling our Technical Support Center. Please have your unit serial number available when you call.

Technical Support	(888) 4ADTRAN
International Technical Support	1-256-963-8716

Installation and Maintenance Support

The ADTRAN Custom Extended Services (ACES) program offers multiple types and levels of installation and maintenance services which allow you to choose the kind of assistance you need. This support is available at:

http://www.adtran.com/aces

For questions, call the ACES Help Desk.

ACES Help Desk	(888) 874-ACES (2237)

Training

The Enterprise Network (EN) Technical Training Department offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN's product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

Training Phone	(800) 615-1176, ext. 7500
Training Fax	(256) 963-6700
Training Email	training@adtran.com

Export Statement

An Export License is required if an ADTRAN product is sold to a Government Entity outside of the EU+8 (Austria, Australia, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom). This requirement is per DOC/BIS ruling G030477 issued 6/6/03. This product also requires that the Exporter of Record file a semi-annual report with the BXA detailing the information per EAR 740.17(5)(e)(2).

DOC - Department of Commerce
BIS - Bureau of Industry and Security
BXA - Bureau of Export Administration

Table of Contents

REFERENCE GUIDE INTRODUCTION

This manual provides information about the commands that are available with all of the NetVanta Series units.

This manual provides information about the commands that are available with NetVanta 5000 Series units. For a list of all of the commands available through the CLI, see 61950860L1-35L (All Products).

If you are new to the ADTRAN Operating System’s (AOS) Command Line Interface (CLI), take a few moments to review the information provided in the section which follows (*CLI Introduction*).

If you are already familiar with the CLI and you need information on a specific command or group of commands, proceed to *Command Descriptions* on page 14 of this guide.

CLI INTRODUCTION

This portion of the Command Reference Guide is designed to introduce you to the basic concepts and strategies associated with using the AOS CLI.

Accessing the CLI from your PC

All products using the AOS are initially accessed by connecting a VT100 terminal (or terminal emulator) to the **CONSOLE** port located on the rear panel of the unit using a standard DB-9 (male) to DB-9 (female) serial cable. Configure the VT100 terminal or terminal emulation software to the following settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

NOTE *For more details on connecting to your unit, refer to the Quick Configuration Guides and Quick Start Guides located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Understanding Command Security Levels

The ADTRAN CLI has two command security levels — **Basic** and **Enable**. Both levels support a specific set of commands. For example, all interface configuration commands are accessible only through the Enable security level. The following table contains a brief description of each level.

Level	Access by...	Prompt	With this level you can...
Basic	beginning an AOS session.	>	• display system information • perform traceroute and ping functions • open a Telnet session
Enable	entering **enable** while in the Basic command security level as follows: >**enable**	#	• manage the startup and running configurations • use the debug commands • enter any of the configuration modes

NOTE *To prevent unauthorized users from accessing the configuration functions of your AOS product, immediately install an Enable-level password. Refer to the Quick Configuration Guides and Quick Start Guides located on the* ***ADTRAN OS Documentation*** *CD provided with your unit for more information on configuring a password.*

Understanding Configuration Modes

The ADTRAN CLI has four configuration modes to organize the configuration commands – Global, Line, Router, and Interface. Each configuration mode supports a set of commands specific to the configurable parameters for the mode. For example, all Frame Relay configuration commands are accessible only through the interface configuration mode (for the virtual Frame Relay interface). The following table contains a brief description of each level.

Mode	Access by...	Sample Prompt	With this mode you can...
Global	entering **config** while at the Enable command security level prompt. For example: >enable #**config term**	(config)#	• set the system's Enable-level password(s) • configure the system global IP parameters • configure the SNMP parameters • enter any of the other configuration modes

Mode	Access by...	Sample Prompt	With this mode you can...
Line	specifying a line (console or Telnet) while at the Global Configuration mode prompt. For example: >enable #config term (config)#**line console 0**	(config-con0)#	• configure the console terminal settings (datarate, login password, etc.) • create Telnet logins and specify their parameters (login password, etc.)
Router	entering **router rip** or **router ospf** while at the Global Configuration mode prompt. For example: >enable #config term (config)#**router rip**	(config-rip)#	• configure RIP or OSPF parameters • suppress route updates • redistribute information from outside routing sources (protocols)
Interface	specifying an interface (T1, Ethernet, Frame Relay, ppp, etc.) while in the Global Configuration mode. For example: >enable #config term (config)#**int eth 0/1**	(config-eth 0/1)# (The above prompt is for the Ethernet **LAN** interface located on the rear panel of the unit.)	• configure parameters for the available LAN and WAN interfaces

Using CLI Shortcuts

The ADTRAN CLI provides several shortcuts which help you configure your AOS product more easily. See the following table for descriptions.

Shortcut	Description
Up arrow key	To re-display a previously entered command, use the up arrow key. Continuing to press the up arrow key cycles through all commands entered starting with the most recent command.
<Tab> key	Pressing the **<Tab>** key after entering a partial (but unique) command will complete the command, display it on the command prompt line, and wait for further input.

Shortcut	**Description**
?	The ADTRAN CLI contains help to guide you through the configuration process. Using the question mark, do any of the following: • Display a list of all subcommands in the current mode. For example: (config-t1 1/1)#**coding ?** ami - Alternate Mark Inversion b8zs - Bipolar Eight Zero Substitution • Display a list of available commands beginning with certain letter(s). For example: (config)#**ip d?** default-gateway dhcp-server domain-lookup domain-name domain-proxy • Obtain syntax help for a specific command by entering the command, a space, and then a question mark (?). The ADTRAN CLI displays the range of values and a brief description of the next parameter expected for that particular command. For example: (config-eth 0/1)#**mtu ?** <64-1500> - MTU (bytes)
<Ctrl + A>	Jump to the beginning of the displayed command line. This shortcut is helpful when using the **no** form of commands (when available). For example, pressing **<Ctrl + A>** at the following prompt will place the cursor directly after the **#**: (config-eth 0/1)#**ip address 192.33.55.6**
<Ctrl + E>	Jump to the end of the displayed command line. For example, pressing **<Ctrl + E>** at the following prompt will place the cursor directly after the **6**: (config-eth 0/1)#**ip address 192.33.55.6**
<Ctrl + U>	Clears the current displayed command line. The following provides an example of the **<Ctrl + U>** feature: (config-eth 0/1)#**ip address 192.33.55.6** (Press **<Ctrl + U>** here) (config-eth 0/1)#
auto finish	You need only enter enough letters to identify a command as unique. For example, entering **int t1 1/1** at the Global configuration prompt provides you access to the configuration parameters for the specified T1 interface. Entering **interface t1 1/1** would work as well, but is not necessary.

Performing Common CLI Functions

The following table contains descriptions of common CLI commands.

Command	Description
do	The **do** command provides a way to execute commands in other command sets without taking the time to exit the current and enter the desired one. The following example shows the **do** command used to view the Frame Relay interface configuration while currently in the T1 interface command set: (config)#**interface t1 1/1** (config-t1 1/1)#**do show interfaces fr 7**
no	To undo an issued command or to disable a feature, enter **no** before the command. For example: **no shutdown t1 1/1**
copy running-config startup-config	When you are ready to save the changes made to the configuration, enter this command. This copies your changes to the unit's nonvolatile random access memory (NVRAM). Once the save is complete, the changes are retained even if the unit is shut down or suffers a power outage.
show running config	Displays the current configuration.
debug	Use the **debug** command to troubleshoot problems you may be experiencing on your network. These commands provide additional information to help you better interpret possible problems. For information on specific debug commands, refer to the section *Enable Mode Command Set* on page 36.
undebug all	To turn off any active debug commands, enter this command.

CAUTION

*The overhead associated with the **debug** command takes up a large portion of your AOS product's resources and at times can halt other processes. It is best to only use the **debug** command during times when the network resources are in low demand (non-peak hours, weekends, etc.).*

Understanding CLI Error Messages

The following table lists and defines some of the more common error messages given in the CLI.

Message	Helpful Hints
%Ambiguous command **%Unrecognized Command**	The command may not be valid in the current command mode, or you may not have entered enough correct characters for the command to be recognized. Try using the **?** command to determine your error. See *Using CLI Shortcuts* on page 10 for more information.
%Invalid or incomplete command	The command may not be valid in the current command mode, or you may not have entered all of the pertinent information required to make the command valid. Try using the **?** command to determine your error. See *Using CLI Shortcuts* on page 10 for more information.
%Invalid input detected at “^” marker	The error in command entry is located where the caret (^) mark appears. Enter a question mark at the prompt. The system will display a list of applicable commands or will give syntax information for the entry.

COMMAND DESCRIPTIONS

This portion of the guide provides a detailed listing of all available commands for the ADTRAN OS CLI (organized by command set). Each command listing contains pertinent information including the default value, a description of all sub-command parameters, functional notes for using the command, and a brief technology review. To search for a particular command alphabetically, use the Index at the end of this document. To search for information on a group of commands within a particular command set, use the linked references given below:

Line Interface Command Sets

Physical Interface Command Sets

Virtual Interface Command Sets

VPN Parameter Command Sets

Routing Protocol Command Sets

Security and Services Command Sets

BASIC MODE COMMAND SET

To activate the Basic mode, simply log in to the unit. After connecting the unit to a VT100 terminal (or terminal emulator) and activating a terminal session, the following prompt displays:

>

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

enable on page 17
logout on page 18
ping <address> on page 19
show clock on page 21
show snmp on page 22
show version on page 23
telnet <address> on page 24
traceroute <address> on page 25

enable

Use the **enable** command (at the Basic Command mode prompt) to enter the Enable Command mode. Use the **disable** command to exit the Enable Command mode. Refer to *Enable Mode Command Set* on page 36 for more information.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The Enable Command mode provides access to operating and configuration parameters and should be password protected to prevent unauthorized use. Use the **enable password** command (found in the Global Configuration mode) to specify an Enable Command mode password. If the password is set, access to the Enable Commands (and all other "privileged" commands) is only granted when the correct password is entered. Refer to *enable password [md5] <password>* on page 335 for more information.

Usage Examples

The following example enters the Enable Command mode and defines an Enable Command mode password:

```
>enable
#configure terminal
(config)#enable password ADTRAN
```

At the next login, the following sequence must occur:

```
>enable
Password: ******
#
```

logout

Use the **logout** command to terminate the current session and return to the login screen.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the logout command being executed in the Basic mode:

```
>logout

Session now available

Press RETURN to get started.
```

ping *<address>*

Use the **ping** command (at the Basic Command mode prompt) to verify Internet Protocol (IP) network connectivity.

Syntax Description

<address>	Specifies the IP address of the system to ping. Entering the **ping** command with no specified address prompts the user with parameters for a more detailed **ping** configuration. Refer to *Functional Notes* (below) for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.Command was introduced.

Functional Notes

The **ping** command helps diagnose basic IP network connectivity using the Packet InterNet Groper program to repeatedly bounce Internet Control Message Protocol (ICMP) echo-request packets off a system (using a specified IP address). The AOS allows executing a standard **ping** request to a specified IP address or provides a set of prompts to configure a more specific **ping** configuration.

The following is a list of output messages from the **ping** command:

!	Success
-	Destination Host Unreachable
$	Invalid Host Address
X	TTL Expired in Transit
?	Unknown Host
*	Request Timed Out

The following is a list of available extended **ping** fields with descriptions:

Target IP address	Specifies the IP address of the system to ping.
Repeat Count	Specifies the number of ping packets to send to the system (valid range: 1 to 1,000,000).
Datagram Size	Specifies the size (in bytes) of the ping packet (valid range: 1 to 1448).
Timeout in Seconds	Specifies the timeout period after which a ping is considered unsuccessful (valid range: 1 to 5 seconds).
Extended Commands	Specifies whether additional commands are desired for more ping configuration parameters.
Source Address (or interface)	Specifies the IP address to use as the source address in the ECHO_REQ packets.
Data Pattern	Specifies an alphanumeric string to use (the ASCII equivalent) as the data pattern in the ECHO_REQ packets.
Sweep Range of Sizes	Varies the sizes of the ECHO_REQ packets transmitted.
Sweep Min Size	Specifies the minimum size of the ECHO_REQ packet (valid range: 0 to 1448).
Sweep Max Size	Specifies the maximum size of the ECHO_REQ packet (valid range: Sweep Min Size to 1448).
Sweep Interval	Specifies the interval used to determine packet size when performing the sweep (valid range: 1 to 1448).
Verbose Output	Specifies an extended results output.

Usage Examples

The following is an example of a successful **ping** command:

```
>ping
Target IP address:192.168.0.30
Repeat count[1-1000000]:5
Datagram Size [1-1000000]:100
Timeout in seconds [1-5]:2
Extended Commands? [y or n]:n
Type CTRL+C to abort.
Legend: '!' = Success '?' = Unknown host '$' = Invalid host address
    '*' = Request timed out '-' = Destination host unreachable
    'x' = TTL expired in transit

Pinging 192.168.0.30 with 100 bytes of data:
!!!!!
Success rate is 100 percent (5/5) round-trip min/avg/max = 19/20.8/25 ms
```

show clock

Use the **show clock** command to display the system time and date entered using the **clock set** command. Refer to the section *clock set <time> <day> <month> <year>* on page 78 for more information.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays the current time and data from the system clock:

```
>show clock

23:35:07 UTC Tue Aug 20 2002
```

show snmp

Use the **show snmp** command to display the system Simple Network Management Protocol (SNMP) parameters and current status of SNMP communications.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is an example output using the **show snmp** command for a system with SNMP disabled and the default chassis and contact parameters:

```
>show snmp

Chassis: Chassis ID
Contact: Customer Service
0 Rx SNMP packets
  0 Bad community names
  0 Bad community uses
  0 Bad versions
  0 Silent drops
  0 Proxy drops
  0 ASN parse errors
```

show version

Use the **show version** command to display the current AOS version information.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample **show version** output:

```
>show version

AOS version 06.01.00
  Checksum: 1F0D5243 built on Fri Nov 08 13:12:06 2002
  Upgrade key: de76efcfeb4c8eeb6901188475dd0917
Boot ROM version 03.00.18
  Checksum: 7A3D built on: Fri Nov 08 13:12:25 2002
Copyright (c) 1999-2002 ADTRAN Inc.
Serial number C14C6308

UNIT_2 uptime is 0 days 4 hours 59 minutes 43 seconds

System returned to ROM by Warm Start
Current system image file is "030018adv.biz"
Boot system image file is "030018adv.biz"
```

telnet *<address>*

Use the **telnet** command to open a Telnet session (through the AOS) to another system on the network.

Syntax Description

<address>	Specifies the IP address of the remote system.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example opens a Telnet session with a remote system (**10.200.4.15**):

```
>telnet 10.200.4.15

User Access Login

Password:
```

traceroute *<address>*

Use the **traceroute** command to display the Internet Protocol (IP) routes a packet takes to reach the specified destination.

Syntax Description

<address>	Specifies the IP address of the remote system to trace the routes to.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example performs a traceroute on the IP address **192.168.0.1**:

```
#traceroute 192.168.0.1

Type CTRL+C to abort.
Tracing route to 192.168.0.1 over a maximum of 30 hops

  1   22ms  20ms  20ms    192.168.0.65
  2   23ms  20ms  20ms    192.168.0.1
#
```

COMMON COMMANDS

The following section contains descriptions of commands that are common across multiple command sets. These commands are listed in alphabetical order.

alias *<"text">*

Use the **alias** command to populate the ifAlias OID (Interface Table MIB of RFC2863) for all physical and virtual interfaces when using Simple Network Management Protocol (SNMP) management stations.

Syntax Description

<"text">	Describes the interface (for SNMP) using an alphanumeric character string enclosed in quotation marks (limited to 64 characters).

Default Values

No defaults required for this command.

Applicable Command Modes

Applies to all interface mode command sets.

Applicable Platforms

Applies to all AOS products.

Command History

Release 1.1	Command was introduced.

Functional Notes

The ifAlias OID is a member of the ifXEntry object-type (defined in RFC2863) used to provide a non-volatile, unique name for various interfaces. This name is preserved through power cycles. Enter a string (using the **alias** command) which clearly identifies the interface.

Usage Examples

The following example defines a unique character string for the T1 interface:

```
(config)#interface t1 1/1
(config-t1 1/1)#alias "CIRCUIT_ID_23-908-8887-401"
```

Technology Review

Please refer to RFC2863 for more detailed information on the ifAlias display string.

cross-connect *<#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port>*

Use the **cross-connect** command to create a cross-connect map from a created TDM group on an interface to a virtual interface.

> CAUTION *Changing **cross-connect** settings could potentially result in service interruption.*

Syntax Description

<#>	Identifies the cross-connect using a number descriptor or label for (useful in systems that allow multiple cross-connects).
<from interface>	Specifies the interface (physical or virtual) on one end of the cross-connect. Enter **cross-connect 1 ?** for a list of valid interfaces.
<slot/port>	Used when a physical interface is specified in the <*from interface*> subcommand (For example: specifying the T1 port of a T1 module would be **t1 1/1**).
<tdm-group#>	Specifies which configured TDM group to use for this cross-connect. This subcommand only applies to T1 physical interfaces.
<to interface>	Specifies the virtual interface on the other end of the cross-connect. Use the **?** to display a list of valid interfaces.
<slot/port>	Used when a physical interface is specified in the <*to interface*> subcommand. (For example, specifying the primary T1 port of a T1 module would be **t1 1/1**).

Default Values

By default, there are no configured cross-connects.

Applicable Platforms

Applies to all AOS products

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the E1 interface.

Functional Notes

Cross-connects provide the mechanism for connecting a configured virtual (layer 2) endpoint with a physical (layer 1) interface. Supported layer 2 protocols include Frame Relay and point-to-point protocol (PPP).

Usage Examples

The following example creates a Frame Relay endpoint and connects it to the T1 1/1 physical interface:

1. Create the Frame Relay virtual endpoint and set the signaling method:

```
(config)# interface frame-relay 1
(config-fr 1)# frame-relay lmi-type cisco
```

2. Create the sub-interface and configure the PVC parameters (including DLCI and IP address):

```
(config-fr 1)# interface fr 1.1
(config-fr 1.1)# frame-relay interface-dlci 17
(config-fr 1.1)# ip address 168.125.33.252 255.255.255.252
```

3. Create the TDM group of 12 DS0s (64K) on the T1 physical interface:
(THIS STEP IS ONLY VALID FOR T1 INTERFACES.)

```
(config)# interface t1 1/1
(config-t1 1/1)# tdm-group 1 timeslots 1-12 speed 64
(config-t1 1/1)# exit
```

4. Connect the Frame Relay sub-interface with port T1 1/1:

```
(config)# cross-connect 1 t1 1/1 1 fr 1
```

Technology Review

Creating an endpoint that uses a layer 2 protocol (such as Frame Relay) is generally a four-step process:

Step 1:

Create the Frame Relay virtual endpoint (using the **interface frame-relay** command) and set the signaling method (using the **frame-relay lmi-type** command). Also included in the Frame Relay virtual endpoint are all the applicable Frame Relay timers logging thresholds, encapsulation types, etc. Generally, most Frame Relay virtual interface parameters should be left at their default state. For example, the following creates a Frame Relay interface labeled **7** and sets the signaling method to **ansi**.

```
(config)# interface frame-relay 7
(config-fr 7)# frame-relay lmi-type ansi
```

Step 2:

Create the sub-interface and configure the PVC parameters. Using the sub-interface, apply access policies to the interface, create bridging interfaces, configure dial-backup, assign an IP address, and set the PVC data-link control identifier (DLCI). For example, the following creates a Frame Relay sub-interface labeled **22,** sets the DLCI to **30,** and assigns an IP address of **193.44.69.253** to the interface.

```
(config-fr 7)# interface fr 7.22
(config-fr 7.22)# frame-relay interface-dlci 30
(config-fr 7.22)# ip address 193.44.69.253 255.255.255.252
```

Step 3: (VALID ONLY FOR T1 INTERFACES)

Specify the group of DS0s used for signaling on the T1 interface by creating a TDM group. Group any number of contiguous DS0s together to create a data pipe for layer 2 signaling. Also use the **tdm-group** command to specify the per-DS0 signaling rate on the interface. For example, the following creates a TDM group labeled **9** containing 20 DS0s (each DS0 having a data rate of 56 kbps).

```
(config)# interface t1 1/1
(config-t1 1/1)# tdm-group 9 timeslots 1-20 speed 56
(config-t1 1/1)# exit
```

Step 4:

Make the association between the layer 2 endpoint and the physical interface using the **cross-connect** command. Supported layer 2 protocols include Frame Relay and point-to-point protocol (PPP). For example, the following creates a cross-connect (labeled **5**) to make an association between the Frame Relay virtual interface (**fr 7**) and the TDM group configured on interface t1 1/1 (**tdm-group 9**).

```
(config)# cross-connect 5 t1 1/1 9 fr 7
```

description *<text>*

Use the **description** command to identify the specified interface (for example, circuit ID, contact information, etc.).

Syntax Description

<text>	Identifies the specified interface using up to 80 alphanumeric characters.

Default Values

No defaults required for this command.

Applicable Command Modes

Applies to all interface mode command sets.

Applicable Platforms

Applies to all AOS products.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enters comment information using the **description** command:

```
(config)#interface t1 1/1
(config-t1 1/1)#description This is the Dallas office T1
```

do

Use the **do** command to execute any AOS command, regardless of the active configuration mode. It provides a way to execute commands in other modes without taking the time to exit the current mode and enter the desired one.

Syntax Description

No subcommands.

Default Values

No defaults required for this command.

Applicable Command Modes

Applies to all mode command sets.

Applicable Platforms

Applies to all AOS products.

Command History

Release 2.1	Command was introduced.

Functional Notes

Use the **do** command to view configurations or interface states after configuration changes are made without exiting to the Enable mode.

Usage Examples

The following example shows the **do** command used to view the Frame Relay interface configuration while currently in the T1 Interface Configuration mode:

```
(config)#interface t1 1/1
(config-t1 1/1)#do show interfaces fr 7
fr 7 is ACTIVE
  Signaling type is ANSI signaling role is USER
  Polling interval is 10 seconds full inquiry interval is 6 polling intervals
Output queue: 0/0 (highest/drops)
    0 packets input 0 bytes
    0 pkts discarded 0 error pkts 0 unknown protocol pkts
    0 packets output 0 bytes
    0 tx pkts discarded 0 tx error pkts
```

end

Use the **end** command to exit the current configuration mode and enter the Enable Security mode.

> NOTE *When exiting the Global Configuration mode, remember to perform a* ***copy running-config startup-config*** *to save all configuration changes.*

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Command Modes

Applies to all mode command sets except Basic mode.

Applicable Platforms

Applies to all AOS products.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the **end** command being executed in the T1 Interface Configuration mode:

```
(config-t1 1/1)#end
#
```

#- Enable Security mode command prompt

exit

Use the **exit** command to exit the current configuration mode and enter the previous one. For example, using the **exit** command in an interface configuration mode will activate the Global Configuration mode. When using the **exit** command in the Basic mode, the current session will be terminated.

> *When exiting the Global Configuration mode, remember to perform a* ***copy running-config startup-config*** *to save all configuration changes.*

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Command Modes

Applies to all mode command sets.

Applicable Platforms

Applies to all AOS products.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the **exit** command being executed in the Global Configuration mode:

```
(config)#exit
#
```

#- Enable Security mode command prompt

shutdown

Use the **shutdown** command to disable the interface (both physical and virtual) so that no data will be passed through. Use the **no** form of this command to turn on the interface and allow it to pass data. By default, all interfaces are disabled.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are disabled.

Applicable Command Modes

Applies to all interface mode command sets.

Applicable Platforms

Applies to all AOS products.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example administratively disables the modem interface:

```
(config)#interface modem 1/2
(config-modem 1/2)#shutdown
```

ENABLE MODE COMMAND SET

To activate the Enable mode, enter the **enable** command at the Basic mode prompt. (If an enable password has been configured, a password prompt will display.) For example:

```
>enable
Password: XXXXXXX
#
```

The following command is common to multiple command sets and is covered in a centralized section of this guide. For more information, refer to the section listed below:

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

clear commands begin on page 38

clock auto-correct-dst on page 76

clock no-auto-correct-dst on page 77

clock set <time> <day> <month> <year> on page 78

clock timezone <text> on page 79

configure [memory | network | overwrite-network | terminal] on page 82

copy <source> <destination> on page 83

copy console <filename> on page 84

copy flash <destination> on page 85

copy <filename> interface <interface> <slot/port> on page 86

copy tftp <destination> on page 87

copy xmodem <destination> on page 88

debug commands begin on page 89

dir on page 141

dir [<input> | flash | flash <input>] on page 142

disable on page 143

enable on page 144

erase [<filename> | startup-config] on page 145

events on page 146

exception report generate on page 147

logout on page 148

ping <address> on page 149

reload [cancel | in <delay>] on page 151

show commands begin on page 152

clear access-list *<listname>*

Use the **clear access-list** command to clear all counters associated with all access lists (or a specified access list).

Syntax Description

<listname>	Optional*.* Specifies the name (label) of an access list.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example clears all counters for the access list labeled **MatchAll**:

```
>enable
#clear access-list MatchAll
```

clear arp-cache

Use the **clear arp-cache** command to remove all dynamic entries from the Address Resolution Protocol (ARP) cache table.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example removes all dynamic entries from the ARP cache:

```
>enable
#clear arp-cache
```

clear arp-entry *<address>*

Use the **clear arp-entry** command to remove a single entry from the Address Resolution Protocol (ARP) cache.

Syntax Description

<address>	Specifies the IP address of the entry to remove.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example removes the entry for 10.200.4.56 from the ARP cache:

```
>enable
#clear arp-entry 10.200.4.56
```

clear bridge *<group#>*

Use the **clear bridge** command to clear all counters associated with bridging (or for a specified bridge-group).

Syntax Description

<group#>	Optional. Specifies a single bridge group (1 to 255).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example clears all counters for bridge group 17:

```
>enable
#clear bridge 17
```

clear buffers max-used

Use the **clear buffers max-used** command to clear the maximum-used statistics for buffers displayed in the **show memory heap** command.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example clears the maximum-used buffer statics:

```
>enable
#clear buffers max-used
```

clear counters [*<interface> <interface id>*]

Use the **clear counters** command to clear all interface counters (or the counters for a specified interface).

Syntax Description

<interface>	Optional. Specifies a single interface. Enter **clear counters ?** or **show interface ?** for a complete list of interfaces.
<interface id>	Optional. Specifies the ID of the specific interface to clear (e.g., 1 for port channel 1).

Default Values

No default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.

Usage Examples

The following example clears all counters associated with the Ethernet 0/1 interface:

```
>enable
#clear counters ethernet 0/1
```

clear crypto ike sa *<policy priority>*

Use the **clear crypto ike sa** command to clear existing IKE security associations (SAs), including active ones.

Syntax Description

<policy priority>	Optional. Clears out all existing IKE SAs associated with the designated policy priority. This number is assigned using the **crypto ike policy** command. Refer to *crypto ike* on page 322 for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example clears the entire database of IKE SAs (including the active associations):

```
>enable
#clear crypto ike sa
```

clear crypto ipsec sa

Use the **clear crypto ipsec sa** command to clear existing IPSec security associations (SAs), including active ones.

Variations of this command include the following:

clear crypto ipsec sa
clear crypto ipsec sa entry *<ip address>* **ah** *<SPI>*
clear crypto ipsec sa entry *<ip address>* **esp** *<SPI>*
clear crypto ipsec sa map *<map name>*
clear crypto ipsec sa peer *<ip address>*

Syntax Description

entry *<ip address>*	Clears only the SAs related to a certain destination IP address.
ah *<SPI>*	Clears only a portion of the SAs by specifying the authentication header (AH) protocol and a security parameter index (SPI). You can determine the correct SPI value using the **show crypto ipsec sa** command.
esp *<SPI>*	Clears only a portion of the SAs by specifying the encapsulating security payload (ESP) protocol and an SPI. You can determine the correct SPI value using the **show crypto ipsec sa** command.
map *<map name>*	Clears only the SAs associated with the crypto map name given.
peer *<ip address>*	Clears only the SAs associated with the far-end peer IP address given.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example clears all IPSec SAs:

```
> enable
#clear crypto ipsec sa
```

The following example clears the IPSec SA used for ESP traffic with the SPI of 300 to IP address 63.97.45.57:

```
> enable
#clear crypto ipsec sa entry 63.97.45.57 esp 300
```

clear dump-core

The **clear dump-core** command clears diagnostic information appended to the output of the **show version** command. This information results from an unexpected unit reboot.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example clears the entire database of IKE SAs (including the active associations):

```
>enable
#clear dump-core
```

clear event-history

Use the **clear event-history** command to clear all messages logged to the local event-history.

> CAUTION
>
> *Messages cleared from the local event-history (using the **clear event-history** command) are no longer accessible.*

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example clears all local event-history messages:

```
>enable
#clear event-history
```

clear host [* | *<hostname>*]

Use the **clear host** command to clear a hostname when using the Domain Naming System (DNS) proxy.

Syntax Description

*****	Clears all dynamic hosts.
<hostname>	Clears a specific host name.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example clears all dynamic hostnames:

```
>enable
#clear host *
```

clear ip bgp [* | *<as-number>* | *<ip address>*] [in | out | soft]

Use the **clear ip bgp** command to clear BGP neighbors as specified.

Syntax Description

*****	Clears all BGP neighbors.
<as-number>	Clears all BGP neighbors with the specified autonomous system (AS) number. Range is 1 to 65,535.
<ip address>	Clears the BGP neighbor with the specified IP address.
in	Causes a “soft” reset inbound with a neighbor, reprocessing routes advertised by that neighbor.
out	Causes a “soft” reset outbound with a neighbor, re-sending advertised routes to that neighbor.
soft	Causes a “soft” reset both inbound and outbound.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

The **clear ip bgp** command must be issued to re-initialize the BGP process between the peers matching the given arguments. Most neighbor changes, including changes to prefix-list filters, do not take effect until the **clear** command is issued. A hard reset clears the TCP connection with the specified peers, which results in clearing the table. This method of clearing is disruptive and causes peer routers to record a route flap for each route.

The **out** version of this command provides a soft reset out to occur by causing all routes to be re-sent to the specified peer(s). TCP connections are not torn down, so this method is less disruptive. Output filters/policies are re-applied before sending the update.

The **in** version of this command provides a soft reset in to occur by allowing the router to receive an updated table from a peer without tearing down the TCP connection. This method is less disruptive and does not count as a route flap. Currently, all of the peer's routes are stored permanently, even if they are filtered by a prefix list. The command causes the peer's routes to be reprocessed with any new parameters.

Usage Examples

The following example causes a hard reset with peers with an AS number of 101:

```
>enable
#clear ip bgp 101
```

clear ip cache

Use the **clear ip cache** command to delete cache table entries.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example removes all entries from the cache table:

```
>enable
#clear ip cache
```

clear ip dhcp-server binding [* | *<ip address>*]

Use the **clear ip dhcp-server binding** command to clear Dynamic Host Configuration Protocol (DHCP) server binding entries from the database.

Syntax Description

*****	Clears all automatic binding entries.
<ip address>	Clears a specific binding entry. Enter the source IP address (format is A.B.C.D).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Functional Notes

A DHCP server binding represents an association between a MAC address and an IP address that was offered by the unit to a DHCP client (i.e., most often a PC). Clearing a binding allows the unit to offer that IP address again, should a request be made for one.

Usage Examples

The following example clears a DHCP server binding for the IP address **125.25.47.4**:

```
>enable
#clear ip dchp-server binding 125.25.47.4
```

clear ip igmp group [*<group-address>* | *<interface>*]

Use the **clear ip igmp group** command to clear entries from the Internet Group Management Protocol (IGMP) tables. If no address or interface is specified, all non-static IGMP groups are cleared with this command.

Syntax Description

<*group-address*>	Optional. Specifies the multicast IP address of the multicast group.
<*interface*>	Optional. Designates the display of parameters for a specific interface (in the format type slot/port). For example: **eth 0/1**.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include HDSL and tunnel interfaces.

Usage Examples

The following example shows output for the **show igmp groups** command before and after a **clear ip igmp group** command is issued. This example clears the IGMP entry that was registered dynamically by a host. Interfaces that are statically joined are not cleared:

```
#show ip igmp groups
IGMP Connected Group Membership
Group Address
Interface
Uptime
Expires
Last Reporter
172.0.1.50
Loopback100
01:22:59
00:02:46
172.23.23.1
172.1.1.1
Ethernet0/1
```

```
00:00:14
00:02:45
1.1.1.2
172.1.1.1
Loopback100
01:22:59
00:02:46
172.23.23.1
#clear ip igmp group

#show ip igmp groups
IGMP Connected Group Membership
Group Address
Interface
Uptime
Expires
Last Reporter
```

This version of the command clears all dynamic groups that have the specified output interface (Ethernet 0/1):

```
#clear ip igmp group ethernet 0/1
```

This version of the command clears the specified group on all interfaces where it is dynamically registered:

```
#clear ip igmp group 172.1.1.1
```

clear ip ospf [process | redistribution]

Use the **clear ip ospf** command to reset open shortest path first (OSPF) information.

Syntax Description

process	Restarts the OSPF process.
redistribution	Refreshes routes redistributed over OSPF.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example resets the OSPF process:

```
>enable
#clear ip ospf process
```

clear ip policy-sessions

Use the **clear ip policy-sessions** command to clear policy class sessions. You may clear all the sessions or a specific session. Use the **show ip policy-sessions** command to view a current session listing. The following lists the complete syntax for the **clear ip policy-sessions** commands:

clear ip policy-sessions

clear ip policy-sessions *<classname>* **[ahp | esp | gre | icmp | tcp | udp |** *<protocol>***]** *<source ip>* *<source port><dest ip><dest port>*

clear ip policy-sessions *<classname>* **[ahp | esp | gre | icmp | tcp | udp |** *<protocol>***]** *<source ip>* *<source port><dest ip><dest port>* **[destination | source]** *<nat ip><nat port>*

Syntax Description

<classname>	Alphanumeric descriptor for identifying the configured access policy (access policy descriptors are not case-sensitive).
ahp	Specifies authentication header protocol (AHP).
esp	Specifies encapsulating security payload protocol (ESP).
gre	Specifies general routing encapsulation protocol (GRE).
icmp	Specifies Internet control message protocol (ICMP) protocol.
tcp	Specifies transmission control protocol (TCP).
udp	Specifies universal datagram protocol (UDP).
<protocol>	Specifies protocol (valid range: 0 to 255).
<source ip>	Specifies the source IP address (format is A.B.C.D).
<source port>	Specifies the source port (in hex format AHP, ESP, and GRE; decimal for all other protocols).
<dest ip>	Specifies the destination IP address (format is A.B.C.D).
<dest port>	Specifies the destination port (in hex format for AHP, ESP, and GRE; decimal for all other protocols).
[destination | source]	For NAT sessions, this specifies whether to select a NAT source or NAT destination session.
<nat ip>	For NAT sessions, this specifies the NAT IP address (format is A.B.C.D).
<nat port>	For NAT sessions, this specifies the NAT port (in hex format for AHP, ESP, and GRE; decimal for all other protocols).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The second half of this command, beginning with the source IP address may be copied and pasted from a row in the **show ip policy-sessions** table for easier use.

Usage Examples

The following example clears the Telnet association (TCP port **23**) for policy class **pclass1** with source IP address **192.22.71.50** and destination **192.22.71.130**:

```
>enable
#clear ip policy-sessions pclass1 tcp 192.22.71.50 23 192.22.71.130 23
```

clear ip policy-stats *<classname>* entry *<policy class #>*

Use the **clear ip policy-stats** command to clear statistical counters for policy classes.

Syntax Description

<classname>	Optional. Specifies the policy class to clear. If no policy class is specified, statistics are cleared for all policies.
entry *<policy class #>*	Optional. Use this keyword to clear statistics of a specific policy class entry.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example clears statistical counters for all policy classes:

```
>enable
#clear ip policy-stats
```

The following example clears statistical counters for the policy class **MatchALL**:

```
>enable
#clear ip policy-stats MatchALL
```

clear ip prefix-list *<listname>*

Use the **clear ip prefix-list** command to clear the IP prefix list hit count shown in the **show ip prefix-list detail** command output. Refer to *show ip prefix-list [detail | summary] <listname>* on page 226 for more information.

Syntax Description

<listname>	Specifies hit count statistics of the IP prefix list to clear.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example clears the hit count statistics for prefix list **test**:

```
>enable
#clear ip prefix-list test
```

clear ip route [** | *<ip address> <subnet mask>*]

Use the **clear ip route** command to remove all learned routes from the IP route table. Static and connected routes are not cleared by this command.

Syntax Description

**	Deletes all destination routes.
<ip address>	Specifies the IP address of the destination routes to be deleted.
<subnet mask>	Specifies the subnet mask of the destination routes to be deleted

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example removes all learned routes from the route table:

```
>enable
#clear ip route **
```

clear lldp counters

Use the **clear lldp counters** command to reset all local loop demarkation point (LLDP) packet counters to zero on all interfaces.

Syntax Description

No subcommands.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example resets all LLDP counters:

```
>enable
#clear lldp counters
```

clear lldp counters interface *<interface>*

Use the **clear lldp counters interface** command to reset all local loop demarkation point (LLDP) packet counters to zero for a specified interface.

Syntax Description

<interface>	Clears the information for the specified interface. Type **clear lldp counters interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example resets the counters on PPP interface 1:

```
>enable
#clear lldp counters interface ppp 1
```

clear lldp neighbors

Use the **clear lldp neighbors** command to remove all neighbors from this unit's database. As new local loop demarkation point (LLDP) packets are received, the database will contain information about neighbors included in those frames.

Syntax Description

No subcommands.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command generates output indicating the names of any neighbors deleted from the database and the name of the interface on which the neighbor was learned.

Usage Examples

The following example clears LLDP neighbor **Switch_1** from the Ethernet interface 0/7:

```
>enable
#clear lldp neighbors
LLDP: Deleted neighbor "Switch_1" on interface eth 0/7
#
```

clear pppoe *<interface id>*

Use the **clear pppoe** command to terminate the current PPPoE client session and cause the AOS to attempt to re-establish the session.

Syntax Description

<interface id>	Specifies the PPP interface ID number to clear.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example ends the current PPPoE client session for ppp 1:

```
>enable
#clear pppoe 1
```

clear processes cpu max

Use the **clear processes cpu max** command to clear the maximum CPU usage statistic which is displayed in the **show process cpu** command output.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example resets the CPU maximum usage statistics:

```
>enable
#clear process cpu max
```

clear qos map

Use the **clear qos map** command to clear the statistics for all defined quality of service (QoS) maps or to view detailed information for maps meeting user-configured specifications.

Variations of this command include the following:

clear qos map <*map name*>
clear qos map <*map name*> <*sequence number*>
clear qos map interface <*interface id*>

Syntax Description

<*map name*>	Specifies the name of a defined QoS map.
<*sequence number*>	Specifies one of the map's defined sequence numbers.
<*interface*>	Specifies an interface for which to clear QoS map statistics (for just that interface). Type **clear qos map interface ?** for a complete list of applicable interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example clears statistics for all defined QoS maps:

#**clear qos map**

The following example clears statistics for all entries in the **priority** QoS map:

#**clear qos map priority**

The following example clears statistics in entry **10** of the **priority** QoS map:

#**clear qos map priority 10**

The following example clears QoS statistics for a specified interface:

#**clear qos map interface frame-relay 1**

*The **clear counters** command clears ALL interface statistics (including QoS map interface statistics).*

clear route-map counters *<map>*

Use the **clear route-map counters** command to reset route map hit counters.

Syntax Description

<map>	Specifies specific route map to be cleared.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears all route map counters:

```
>enable
#clear route-map counters
```

clear sip location [** | *<username>*]

Use the **clear sip location** command to clear session initiation protocol (SIP) location database statistics.

Syntax Description

**	Clears all dynamic location entries.
<username>	Specifies specific username to clear.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example deletes all dynamic location entries:

```
>enable
#clear sip location **
```

clear sip user-registration

Use the **clear sip user-registration** command to clear local session initiation protocol (SIP) server registration information.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears all SIP server registration information:

```
>enable
#clear sip user-registration
```

clear spanning-tree counters [interface *<interface id>*]

The **clear spanning-tree counters** command clears the following counts: BPDU transmit, BPDU receive, and number of transitions to forwarding state.

Syntax Description

interface *<interface id>*	Optional. Specifies a single interface. Enter **clear spanning-tree counters ?** for a complete list of interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example clears the spanning tree counters for Ethernet 0/10:

```
>enable
#clear spanning-tree counters interface eth 0/10
```

clear spanning-tree detected-protocols [interface *<interface id>*]

Use the **clear spanning-tree detected-protocols** command to restart the protocol migration process.

Syntax Description

interface *<interface id>*	Optional. Specifies a valid interface to clear. Type **clear spanning-tree detected-protocols interface ?** for a complete list of applicable interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The switch has the ability to operate using the rapid spanning-tree protocol or the legacy 802.1D version of spanning-tree. When a BPDU (bridge protocol data unit) of the legacy version is detected on an interface, the switch automatically regresses to using the 802.1D spanning-tree protocol for that interface. Issue the **clear spanning-tree detected-protocols** command to return to rapid spanning-tree operation.

Usage Examples

The following example re-initiates the protocol migration process on Ethernet interface 0/3:

```
>enable
#clear spanning-tree detected-protocols interface ethernet 0/3
```

The following example re-initiates the protocol migration process on all interfaces:

```
>enable
#clear spanning-tree detected-protocols
```

clear tacacs+ statistics

Use the **clear tacacs+ statistics** command to delete all terminal access controller access control system (TACACS+) protocol statistics.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example clears all TACACS+ protocol statistics:

```
>enable
#clear tacacs+ statistics
```

clear user [console *<user number>* | ssh *<user number>* | telnet *<user number>*]

Use the **clear user** command to detach a user from a given line.

Syntax Description

console *<user number>*	Detaches a specific console user. Valid range is 0 to 1.
ssh *<user number>*	Detaches a specific secure shell (SSH) user. Valid range is 0 to 4.
telnet *<user number>*	Detaches a specific Telnet user. Valid range is 0 to 5.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example detaches the **console 1** user:

```
>enable
#clear user console 1
```

clock auto-correct-dst

The **clock auto-correct-dst** command allows the automatic one-hour correction for Daylight Saving Time (DST). Use the **clock no-auto-correct-dst** command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example allows for automatic DST correction:

```
>enable
#clock auto-correct-dst
```

clock no-auto-correct-dst

The **clock no-auto-correct-dst** command allows you to override the automatic one-hour correction for Daylight Saving Time (DST).

Syntax Description

No subcommands.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

Many time zones include an automatic one-hour correction for daylight saving time at the appropriate time. You may override it at your location using this command.

Usage Examples

The following example overrides the one-hour offset for DST:

```
>enable
#clock no-auto-correct-dst
```

clock set *<time> <day> <month> <year>*

Use the **clock set** command to configure the system software clock. For the command to be valid, all fields must be entered. Refer to the *Usage Example* below for an example.

Syntax Description

<time>	Sets the time (in 24-hour format) of the system software clock in the format HH:MM:SS (hours:minutes:seconds).
<day>	Sets the current day of the month (valid range: 1 to 31).
<month>	Sets the current month (valid range: January to December). You need only enter enough characters to make the entry unique. This entry is not case-sensitive.
<year>	Sets the current year (valid range: 2000 to 2100).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sets the system software clock for 3:42 pm, August 22 2004:

```
>enable
#clock set 15:42:00 22 Au 2004
```

clock timezone *<text>*

The **clock timezone** command sets the unit's internal clock to the timezone of your choice. This setting is based on the difference in time (in hours) between Greenwich Mean Time (GMT) or Central Standard Time (CST) and the timezone for which you are setting up the unit. Use the **no** form of this command to disable this feature.

Syntax Description

Subcommands are specified in the *Functional Notes* section for this command.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was expanded to include clock timezone 0.

Functional Notes

The following list shows sample cities and their timezone codes.

```
clock timezone +1-Amsterdam
clock timezone +1-Belgrade
clock timezone +1-Brussels
clock timezone +1-Sarajevo
clock timezone +1-West-Africa
clock timezone +10-Brisbane
clock timezone +10-Canberra
clock timezone +10-Guam
clock timezone +10-Hobart
clock timezone +10-Vladivostok
clock timezone +11
clock timezone +12-Auckland
clock timezone +12-Fiji
clock timezone +13
clock timezone +2-Athens
clock timezone +2-Bucharest
clock timezone +2-Cairo
clock timezone +2-Harare
clock timezone +2-Helsinki
clock timezone +2-Jerusalem
clock timezone +3-Baghdad
clock timezone +3-Kuwait
clock timezone +3-Moscow
clock timezone +3-Nairobi
clock timezone +3:30
clock timezone +4-Abu-Dhabi
clock timezone +4-Baku
clock timezone +4:30
clock timezone +5-Ekaterinburg
clock timezone +5-Islamabad
clock timezone +5:30
clock timezone +5:45
clock timezone +6-Almaty
clock timezone +6-Astana
clock timezone +6-Sri-Jay
clock timezone +6:30
clock timezone +7-Bangkok
clock timezone +7-Kranoyarsk
clock timezone +8-Bejing
clock timezone +8-Irkutsk
clock timezone +8-Kuala-Lumpur
clock timezone +8-Perth
clock timezone +8-Taipei
clock timezone +9-Osaka
clock timezone +9-Seoul
clock timezone +9-Yakutsk
clock timezone +9:30-Adelaide
clock timezone +9:30-Darwin
clock timezone -1-Azores
clock timezone -1-Cape-Verde
clock timezone -10
clock timezone -11
clock timezone -12
clock timezone -2
clock timezone -3-Brasilia
clock timezone -3-Buenos-Aires
clock timezone -3-Greenland
clock timezone -3:30
clock timezone -4-Atlantic-Time
clock timezone -4-Caracus
clock timezone -4-Santiago
clock timezone -5
clock timezone -5-Bogota
clock timezone -5-Eastern-Time
clock timezone -6-Central-America
clock timezone -6-Central-Time
clock timezone -6-Mexico-City
clock timezone -6-Saskatchewan
clock timezone -7-Arizona
clock timezone -7-Mountain-Time
clock timezone -8
clock timezone -9
clock timezone 0
clock timezone GMT-Casablanca
clock timezone GMT-Dublin
```

Usage Examples

The following example sets the timezone for Santiago, Chile.

```
>enable
#clock timezone -4-Santiago
```

configure [memory | network | overwrite-network | terminal]

Use the **configure** command to enter the Global Configuration mode or to configure the system from memory. Refer to *Global Configuration Mode Command Set* on page 281 for more information.

Syntax Description

memory	Configures the active system with the commands located in the default configuration file stored in NVRAM.
network	Configures the system from a TFTP network host.
overwrite-network	Overwrites NVRAM memory from a TFTP network host.
terminal	Enters the Global Configuration mode.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enters the Global Configuration mode from the Enable mode:

```
>enable
#configure terminal
(config)#
```

copy *<source> <destination>*

Use the **copy** command to copy any file from a specified source to a specified destination.

Syntax Description

<source>	Specifies the current location of the file to copy. Valid sources include: **running-config** (current running configuration file), **startup-config** (configuration file located in NVRAM), or a filename (located in FLASH memory).
<destination>	Specifies the destination of the copied file. Valid destinations include: **running-config** (current running configuration file), **startup-config** (configuration file located in NVRAM), or a filename (located in FLASH memory).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example creates a copy of the file **myfile.biz** (located in FLASH memory) and names it **newfile.biz**:

```
>enable
#copy myfile.biz newfile.biz
```

The following example creates a backup copy of the startup configuration file (and places in FLASH memory):

```
>enable
#copy startup-config backup.bak
```

The following example copies the current running-configuration file to the startup configuration file located in NVRAM:

```
>enable
#copy running-config startup-config
```

copy console *<filename>*

Use the **copy console** command to copy the console's input to a text file. To end copying to the text file, type <**Ctrl+D**>. The file will be saved in the AOS root directory.

Syntax Description

<filename>	Specifies destination file for console input.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

The copy console command works much like a line editor. Prior to pressing **<Enter>**, changes can be made to the text on the line. Changes can be made using **<Delete>** and **<Backspace>** keys. The text can be traversed using the arrow keys, **<Ctrl+A>** (to go to the beginning of a line), and **<Ctrl+E>** (to go to the end of a line). To end copying to the text file, type **<Ctrl+D>.** The file will be saved in the AOS root directory. Use the **dir** command to see a list of files in the root directory.

Usage Examples

The following example copies the console input into the file **config** (located in the AOS root directory):

```
>enable
#copy console config
```

copy flash *<destination>*

Use the **copy flash** command to copy a file located in flash memory to a specified destination.

Syntax Description

<destination>	Specifies the destination of the copied file. Valid destinations include **tftp** and **xmodem**.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example copies the contents of the unit's flash memory to a TFTP server:

```
>enable
#copy flash tftp
```

copy *<filename>* interface *<interface> <slot/port>*

Use the **copy interface** command to copy a file to a specified interface.

Syntax Description

<filename>	Specifies file name of source file to copy.
<interface>	Specifies interface to be upgraded.
<slot/port>	Specifies slot and port number of interface.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example upgrades the ADSL interface with the firmware file **configfile**:

```
>enable
#copy configfile interface adsl 0/1
```

copy tftp *<destination>*

Use the **copy tftp** command to copy a file located on a network Trivial File Transfer Protocol (TFTP) server to a specified destination.

Syntax Description

<destination>	Specifies the destination of the file copied from the TFTP server. Valid destinations include: **flash** (FLASH memory), **startup-config** (the configuration file stored in NVRAM), or **running-config** (the current running configuration file). After entering **copy tftp** and specifying a destination, the AOS prompts for the following information:
Address of remote host:	IP address of the TFTP server.
Source filename:	Name of the file to copy from the TFTP server.
Destination filename:	Specifies the filename to use when storing the copied file to FLASH memory. (Valid only for the **copy tftp flash** command.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example copies **myfile.biz** from the TFTP server (10.200.2.4) to flash memory and labels it **newfile.biz**:

```
>enable
#copy tftp flash

Address of remote host?10.200.2.4
Source filename myfile.biz
Destination filename newfile.biz
Initiating TFTP transfer...
Received 45647 bytes.
Transfer Complete!
#
```

copy xmodem *<destination>*

Use the **copy xmodem** command to copy a file (using the XMODEM protocol) to a specified destination. XMODEM capability is provided in terminal emulation software such as HyperTerminal™.

Syntax Description

<destination> Specifies the destination of the copied file.

Valid destinations include: **flash** (FLASH memory), **startup-config** (the configuration file stored in NVRAM), or **running-config** (the current running configuration file).

After entering **copy xmodem** and specifying a destination, the AOS prompts for the following information:

Destination filename: Specifies the filename to use when storing the copied file to FLASH memory. (Valid only for the **copy flash** command.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example copies a .biz file to flash memory and labels it newfile.biz:

```
>enable
#copy xmodem flash
Destination filename newfile.biz
Begin the Xmodem transfer now...
Press CTRL+X twice to cancel
CCCCCC
```

The AOS is now ready to accept the file on the **CONSOLE** port (using the XMODEM protocol). The next step in the process may differ depending on the type of terminal emulation software you are using. For HyperTerminal, you will now select **Transfer** > **Send File** and browse to the file you wish to copy. Once the transfer is complete, information similar to the following is displayed:

```
Received 231424 bytes.
Transfer complete.
```

debug aaa

Use the **debug aaa** command to activate debug messages associated with authentication from the AAA subsystem. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The **debug aaa** events include connection notices, login attempts, and session tracking.

Usage Examples

The following is sample output for this command:

```
>enable
#debug aaa
AAA: New Session on portal 'TELNET 0 (172.22.12.60:4867)'.
AAA: No list mapped to 'TELNET 0'. Using 'default'.
AAA: Attempting authentication (username/password).
AAA: RADIUS authentication failed.
AAA: Authentication failed.
AAA: Closing Session on portal 'TELNET 0 (172.22.12.60:4867)'.
```

debug access-list *<listname>*

Use the **debug access-list** command to activate debug messages (for a specified list) associated with access list operation. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

<listname>	Specifies a configured access list.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The **debug access-list** command provides debug messages to aid in troubleshooting access list issues.

Usage Examples

The following example activates debug messages for the access list labeled **MatchAll**:

```
>enable
#debug access-list MatchAll
```

debug auto-config

Use the **debug auto-config** command to activate debug messages associated auto-config events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The example activates debug messages associated with auto-config events:

```
>enable
#debug auto-config
```

debug bridge

Use the **debug bridge** command to display messages associated with bridge events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates bridge debug messages:

```
>enable
#debug bridge
```

debug chat-interfaces *<chat interface>*

Use the **debug chat-interfaces** command to activate debug messages associated with chat AT command driven interfaces. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

<chat interface>	Specifies the chat interface to debug in slot/port format.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages for the chat interface 0/1:

```
>enable
#debug chat-interfaces 0/1
```

debug crypto [ike | ike negotiation | ike client authentication | ike client configuration | ipsec | pki]

Use the **debug crypto** command to activate debug messages associated with IKE and IPSec functions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

ike	Displays all IKE debug messages.
ike negotiation	Displays only IKE key management debug messages (e.g., handshaking).
ike client authentication	Displays IKE client authentication messages as they occur.
ike client configuration	Displays mode-config exchanges as they take place over the IKE SA. It is enabled independently from the **ike negotiation** debug described previously.
ipsec	Displays all IPSec debug messages.
pki	Displays all public key infrastructure (PKI) debug messages.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.
Release 6.1	Debug pki command introduced.

Usage Examples

The following example activates the IPSec debug messages:

```
>enable
#debug crypto ipsec
```

debug data-call

Use the **debug data-call** command to activate debug messages associated with data call errors and events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with data call errors and events:

```
>enable
#debug data-call
```

debug demand-routing

Use the **debug demand-routing** command to activate debug messages associated with demand routing errors and events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates demand routing error and event messages:

```
>enable
#debug demand-routing
```

debug dial-backup

Use the **debug dial-backup** command to activate debug messages associated with dial-backup operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 2.1	Additional debug messages were implemented for dial-backup operation to ADTRAN's IQ and Express Series products.

Functional Notes

The **debug dial-backup** command activates debug messages to aid in the troubleshooting of dial-backup links.

Usage Examples

The following example activates debug messages for dial-backup operation:

```
>enable
#debug dial-backup
```

debug dialup-interfaces

Use the **debug dialup-interfaces** command to generate debug messages used to aid in troubleshooting problems with all dialup interfaces such as the modem or the BRI cards. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

When enabled, these messages provide status information on incoming calls, dialing and answering progress, etc. These messages also give information on why certain calls are dropped or rejected. It is beneficial to use this command when troubleshooting dial backup (in addition to the **debug dial-backup** command).

Usage Examples

The following example activates the debug messages for dialup interfaces:

```
>enable
#debug dialup-interfaces
```

debug dynamic-dns [verbose]

Use the **debug dynamic-dns** command to display debug messages associated with dynamic domain naming system (DNS). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

verbose	Enables detailed debug messages.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates dynamic DNS debug messages:

```
>enable
#debug dynamic-dns verbose
```

debug firewall

Use the **debug firewall** command to activate debug messages associated with the AOS firewall operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The **debug firewall** command activates debug messages to provide real-time information about the AOS stateful inspection firewall operation.

Usage Examples

The following example activates the debug messages for the AOS stateful inspection firewall:

```
>enable
#debug firewall
```

debug frame-relay [events | llc2 | lmi]

Use the **debug frame-relay** command to activate debug messages associated with the Frame Relay operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

events	Activates debug messages for generic Frame Relay events (such as Frame Relay interface state).
llc2	Activates debug messages for the logical link control layer.
lmi	Activates debug messages for the local management interface (such as DLCI status signaling state, etc.).

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **debug frame-relay** command activates debug messages to aid in the troubleshooting of Frame Relay links.

Usage Examples

The following example activates all possible debug messages associated with Frame Relay operation:

```
>enable
#debug frame-relay events
#debug frame-relay llc2
#debug frame-relay lmi
```

debug frame-relay multilink *<interface>*

Use the **debug frame-relay multilink** command to activate debug messages associated with Frame Relay multilink operation. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

<interface>	Optional. Activates debug messages for the specified interface. Type **debug frame-relay multilink ?** for a complete list of applicable interfaces.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with multilink operation for all Frame Relay interfaces:

```
>enable
#debug frame-relay multilink
```

debug hdlc [errors | verbose]

Use the **debug hdlc** command to activate debug messages associated with the high-level data link control (HDLC) interface. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

errors	Enables protocol error and statistic messages.
verbose	Enables detailed debug messages.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example activates detailed debug messages associated with the HDLC interface:

```
>enable
#debug hdlc verbose
```

debug interface *<interface>*

Use the **debug interface** command to activate debug messages associated with the specified interface. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

<interface>	Activates debug messages for the specified interface. Type **debug interface ?** for a complete list of applicable interfaces.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 6.1	Command was expanded to include T1 and FXS interfaces.
Release 7.1	Command was expanded to include FXO interface.
Release 9.1	Command was expanded to include tunnel interface.

Functional Notes

The **debug interface** command activates debug messages to aid in the troubleshooting of physical interfaces.

Usage Examples

The following example activates all possible debug messages associated with the Ethernet port:

```
>enable
#debug interface ethernet
```

debug interface adsl events

Use the **debug interface adsl events** command to activate debug messages associated with ADSL events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example activates debug messages for ADSL events:

```
>enable
#debug interface adsl events
```

debug ip bgp [events | in | out | keepalives | updates | updates quiet]

Use the **debug ip bgp** command to activate debug messages associated with IP Border Gateway Protocol (BGP). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

events	Displays significant BGP events such as a neighbor state change.
in/out	Displays the same information as **debug ip bgp**, but limits messages to the specified direction (in or out).
keepalives	Displays BGP keepalive packets.
updates	Displays detailed information on BGP updates for all neighbors.
updates quiet	Displays summary information about BGP neighbor updates. (Note: **updates quiet** displays a one-line summary of what **update** displays in 104 lines.)

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

If no arguments are given, the **debug ip bgp** command displays general BGP events such as sent/received message summaries, route processing actions, and results. Keepalive packets are not debugged with this command.

Usage Examples

The following example enables debug messages on general outbound BGP messages and events:

```
>enable
#debug ip bgp out
#07:42:39: BGP OUT 10.15.240.1[2]: Transmitting msg, type=UPDATE (2), len=142
```

debug ip dhcp-client

Use the **debug ip dhcp-client** command to activate debug messages associated with Dynamic Host Configuration Protocol (DHCP) client operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The **debug ip dhcp-client** command activates debug messages to provide information on DHCP client activity in the AOS. The AOS DHCP client capability allows interfaces to dynamically obtain an IP address from a network DHCP server.

Usage Examples

The following example activates debug messages associated with DHCP client activity:

```
>enable
#debug ip dhcp-client
```

debug ip dhcp-server

Use the **debug ip dhcp-server** command to activate debug messages associated with Dynamic Host Configuration Protocol (DHCP) server operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The **debug ip dhcp-server** command activates debug messages to provide information on DHCP server activity in the AOS. The AOS DHCP server capability allows the AOS to dynamically assign IP addresses to hosts on the network.

Usage Examples

The following example activates debug messages associated with DHCP server activity:

```
>enable
#debug ip dhcp-server
```

debug ip dns-client

Use the **debug ip dns-client** command to activate debug messages associated with domain naming system (DNS) client operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **debug ip dns-client** command activates debug messages to provide information on DNS client activity in the AOS. The IP DNS capability allows for DNS-based host translation (name-to-address).

Usage Examples

The following example activates debug messages associated with DNS client activity:

```
>enable
#debug ip dns-client
```

debug ip dns-proxy

Use the **debug ip dns-proxy** command to activate debug messages associated with domain naming system (DNS) proxy operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **debug ip dns-proxy** command activates debug messages to provide information on DNS proxy activity in the AOS. The IP DNS capability allows for DNS-based host translation (name-to-address).

Usage Examples

The following example activates debug messages associated with DNS proxy activity:

```
>enable
#debug ip dns-proxy
```

debug ip icmp [send | recv]

Use the **debug ip icmp** command to show all Internet Control Message Protocol (ICMP) messages as they come into the router or are originated by the router. If an optional keyword (**send** or **recv**) is not used, all results are displayed. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

send	Optional. Displays only ICMP messages sent by the router.
recv	Optional. Displays only ICMP messages received by the router.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example activates the **debug ip icmp** send and receive messages for the AOS:

```
>enable
#debug ip icmp
ICMP SEND: From (0.0.0.0) to (172.22.14.229) Type=8 Code=0 Length=72 Details:echo request
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=0 Code=0 Length=72 Details:echo reply
ICMP SEND: From (0.0.0.0) to (172.22.14.229) Type=8 Code=0 Length=72 Details:echo request
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=0 Code=0 Length=72 Details:echo reply
ICMP RECV: From (172.22.255.200) to (10.100.23.19) Type=11 Code=0 Length=36 Details:TTL equals 0
during transit
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=3 Code=3 Length=36 Details:port
unreachable
ICMP RECV: From (172.22.14.229) to (10.100.23.19) Type=3 Code=3 Length=36 Details:port
unreachable
```

debug ip igmp *<group-address>*

Use the **debug ip igmp** command to enable debug messages for Internet Group Management Protocol (IGMP) transactions (including helper activity). Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

<*group-address*>	Optional. Specifies the IP address of a multicast group.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables IGMP debug messages for the specified multicast group:

```
>enable
#debug ip igmp 224.1.1.1
```

debug ip mrouting

Use the **debug ip mrouting** command to activate debug messages associated with multicast table routing events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following sample activates **ip mrouting** debug messages:

```
>enable
#debug ip mrouting
```

debug ip ospf

Use the **debug ip ospf** command to activate debug messages associated with open shortest path first (OSPF) routing operations. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

adj	Displays OSPF adjacency events.
database-timer	Displays OSPF database timer.
events	Displays OSPF events.
flood	Displays OSPF flooding.
hello	Displays OSPF hello events.
lsa-generation	Displays OSPF link state advertisement (LSA) generation.
packet	Displays OSPF packets.
retransmission	Displays OSPF retransmission events.
spf	Displays OSPF shortest-path-first (SPF) calculations.
tree	Displays OSPF database tree.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is an example of **debug ip ospf** command results:

```
>enable
#debug ip ospf flood
```

```
OSPF: Update LSA: id=c0a8020d rtid=192.168.2.13 area=11.0.0.0 type=1
OSPF: Update LSA: id=0b003202 rtid=11.0.50.2 area=11.0.0.0 type=1
OSPF: Queue delayed ACK lasid=0b003202 lsartid=11.0.50.2 nbr=11.0.50.2
OSPF: Rx ACK lasid=c0a8020d lsartid=192.168.2.13 nbr=11.0.50.2
OSPF: Received LSA ACK LSA_ID=-64.-88.2.13 LSA_RT_ID=-64.-88.2.13
OSPF: Rx ACK lasid=00000000 lsartid=192.168.2.13 nbr=11.0.50.2
OSPF: Received LSA ACK LSA_ID=0.0.0.0 LSA_RT_ID=-64.-88.2.13
OSPF: Sending delayed ACK
OSPF: Update LSA: id=c0a8020d rtid=192.168.2.13 area=11.0.0.0 type=1
OSPF: Flooding out last interface
OSPF: Update LSA: id=0b003202 rtid=11.0.50.2 area=11.0.0.0 type=1
```

debug ip pim-sparse

Use the **debug ip pim-sparse** command to display all protocol-independent multicast (PIM) sparse mode information. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse mode messages:

```
>enable
#debug ip pim-sparse
```

debug ip pim-sparse assert [event | state] *<address>*

Use the **debug ip pim-sparse assert** command to display debug messages associated with protocol-independent multicast (PIM) sparse assert transactions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

event	Displays PIM sparse assert events.
state	Displays PIM sparse assert state changes.
<address>	Specifies group address to filter.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse assert event messages:

```
>enable
#debug ip pim-sparse assert event
```

debug ip pim-sparse hello

Use the **debug ip pim-sparse hello** command to display protocol-independent multicast (PIM) sparse mode hello transactions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates PIM sparse mode hello messages:

```
>enable
#debug ip pim-sparse hello
```

debug ip pim-sparse joinprune [event | state] *<address>*

Use the **debug ip pim-sparse joinprune** command to display protocol-independent multicast (PIM) sparse mode join and prune transactions. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

event	Displays PIM sparse join and prune events.
state	Displays PIM sparse join and prune state changes.
<*address*>	Specifies group address to filter.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates PIM sparse mode messages for all join and prune events and state changes:

```
>enable
#debug ip pim-sparse joinprune
```

debug ip pim-sparse packets [in | out] *<interface> <interface id>*

Use the **debug ip pim-sparse packets** command to display protocol-independent multicast (PIM) sparse mode packet information. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

in	Displays messages for inbound PIM sparse packets
out	Displays messages for outbound PIM sparse packets.
<interface>	Specifies specific interface. Type **debug ip pim-sparse packets [in | out] interface ?** for a list of valid interfaces.
<interface id>	Specifies a valid interface ID.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse packet messages (both inbound and outbound):

```
>enable
#debug ip pim-sparse packets
```

debug ip pim-sparse register [event | state] *<address>*

Use the **debug ip pim-sparse register** command to display protocol-independent multicast (PIM) sparse source registration messages. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

event	Displays PIM sparse register events.
state	Displays PIM sparse register state changes.
<address>	Specifies group address to filter.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates all PIM sparse registeration state changes:

```
>enable
#debug ip pim-sparse register state
```

debug ip policy

Use the **debug ip policy** command to display policy-based routing events. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates policy-based routing event messages:

```
>enable
#debug ip policy
```

debug ip rip [events]

Use the **debug ip rip** command to activate debug messages associated with Routing Information Protocol (RIP) operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

events	Optional. Displays only RIP protocol events.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **debug ip rip** command activates debug messages to provide information on RIP activity in the AOS. RIP allows hosts and routers on a network to exchange information about routes.

Usage Examples

The following example activates debug messages associated with RIP activity:

```
>enable
#debug ip rip
```

debug ip tcp [events]

Use the **debug ip tcp events** command to activate debug messages associated with significant Transmission Control Protocol (TCP) events such as state changes, retransmissions, session aborts, etc., in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

> NOTE *These debug events are logged for packets that are sent or received from the router. Forwarded TCP packets are not included.*

Syntax Description

events	Optional. Displays only TCP protocol events.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

In the **debug ip tcp events** information, TCB stands for TCP task control block. The numbers which sometimes appear next to TCB (e.g., **TCB5** in the following example) represent the TCP session number. This allows you to differentiate debug messages for multiple TCP sessions.

Usage Examples

The following is sample output for this command:

```
>enable
#debug ip tcp events

2003.02.17 07:40:56 IP.TCP EVENTS TCP: Allocating block 5
2003.02.17 07:40:56 IP.TCP EVENTS TCB5: state change: FREE->SYNRCVD
2003.02.17 07:40:56 IP.TCP EVENTS TCB5: new connection from 172.22.75.246:3473 to
10.200.2.201:23
2003.02.17 07:40:56 IP.TCP EVENTS TCB5: state change: SYNRCVD->ESTABLISHED
[172.22.75.246:3473]
2003.02.17 07:41:06 IP.TCP EVENTS TCB5: Connection aborted -- error = RESET
2003.02.17 07:41:06 IP.TCP EVENTS TCB5: De-allocating tcb
```

debug ip tcp md5

Use the **debug ip tcp md5** command to activate debug messages that detail the results of each incoming Transmission Control Protocol (TCP) packet's MD5 authentication with an internal route in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Debug messages will only be generated for TCP ports that have MD5 authentication enabled.

Usage Examples

The following example activates debug messages associated with incoming TCP packet's MD5 authentication:

```
>enable
#debug ip tcp md5
```

debug ip udp

Use the **debug ip udp** command to activate debug messages associated with User Datagram Protocol (UDP) send and receive events in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

NOTE *These debug events are logged for packets that are sent or received from the router. Forwarded UDP packets are not included.*

CAUTION *The overhead associated with this command takes up a large portion of your router's resources and at times can halt other router processes. It is best to only use the command during times when the network resources are in low demand (non-peak hours, weekends, etc.).*

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

In the **debug ip udp** information, the message **no listener** means that there is no service listening on this UDP port (i.e., the data is discarded).

Usage Examples

The following is sample output for this command:

```
>enable
#debug ip udp

2003.02.17 07:38:48 IP.UDP RX: src=10.200.3.236:138, dst=10.200.255.255:138, 229 bytes, no listener
2003.02.17 07:38:48 IP.UDP RX: src=10.200.2.7:138, dst=10.200.255.255:138, 227 bytes, no listener
2003.02.17 07:38:48 IP.UDP RX: src=10.200.201.240:138, dst=10.200.255.255:138, 215 bytes, no listener
```

debug lldp [rx | tx] verbose

Use the **debug lldp** command to display debug output for all local loop demarkation point (LLDP) receive and transmit packets. Use the **no** version of this command to disable it. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

rx	Shows information about received packets.
tx	Shows information about transmitted packets.
verbose	Shows detailed debugging information.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example activates all possible debug messages associated with LLDP operation:

```
>enable
#debug lldp rx
#debug lldp tx
#debug lldp verbose
```

debug port-auth [general | packet [both | rx | tx] | auth-sm | bkend-sm | reauth-sm | supp-sm]

Use the **debug port-auth** command to generate debug messages used to aid in troubleshooting problems during the port authentication process. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

general	Optional. Displays configuration changes to the port authentication system.
packet both	Optional. Displays packet exchange information in both receive and transmit directions.
packet rx	Optional. Displays packet exchange information in the receive-only direction.
packet tx	Optional. Displays packet exchange information in the transmit-only direction.
auth-sm	Optional. Displays AuthPAE-state machine information.
bkend	Optional. Displays backend-state machine information.
reauth-sm	Optional. Displays reauthentication-state machine information.
supp-sm	Optional. Displays supplicant-state machine information.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 1000, 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 9.1	Command was introduced.
Release 10.1	New options were introduced.

Usage Examples

The following example activates port authentication debug information on received packets:

```
>enable
#debug port-auth packet rx
Rcvd EAPOL Start for sess 1 on int eth 0/2
```

debug ppp [authentication | errors | negotiation | verbose]

Use the **debug ppp** command to activate debug messages associated with point-to-point protocol (PPP) operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

authentication	Activates debug messages pertaining to PPP authentication (CHAP, PAP, EAP, etc.).
errors	Activates debug messages that indicate a PPP error was detected (mismatch in negotiation authentication, etc.).
negotiation	Activates debug messages associated with PPP negotiation.
verbose	Activates detailed debug messages for PPP operation.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **debug ppp** command activates debug messages to provide information on PPP activity in the system. PPP debug messages can be used to aid in troubleshooting PPP links.

Usage Examples

The following example activates debug messages associated with PPP authentication activity:

```
>enable
#debug ppp authentication
```

debug pppoe client

Use the **debug pppoe client** command to activate debug messages associated with point-to-point protocol over Ethernet (PPPoE) operation in the AOS. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, and 4000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with PPPoE activity:

```
>enable
#debug pppoe client
```

debug radius

Use the **debug radius** command to enable debug messages from the RADIUS subsystem. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The **debug radius** messages show the communication process with the remote RADIUS servers.

Usage Examples

The following is an example output for the **debug radius** command:

```
>enable
#debug radius

RADIUS AUTHENTICATION: Sending packet to 172.22.48.1 (1645).
RADIUS AUTHENTICATION: Received response from 172.22.48.1.
```

debug sip [cldu | location | manager | registrar *<extension>* | registration *<extension>*]

Use the **debug sip** command to activate debug messages associated with Session Initiation Protocol (SIP) events. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

location	Activates SIP location database event debug messages.
manager	Activates SIP stack manager event debug messages.
proxy	Activates SIP stack proxy event debug messages.
<subsource>	Specifies a specific subsource.
registrar	Activates SIP registrar event debug messages.
<extension>	Specifies a specific extension.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example activates all debug messages associated with SIP stack manager events:

```
>enable
#debug sip stack manager
```

debug sntp

Use the **debug sntp** command to enable debug messages associated with the Simple Network Time Protocol (SNTP). All SNTP packet exchanges and time decisions are displayed with these debugging events enabled. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **debug sntp** command activates debug messages to aid in troubleshooting SNTP protocol issues.

Usage Examples

The following is an example output for the **debug sntp** command:

```
>enable
#debug sntp
#config term
(config)#sntp server timeserver.localdomain

2002.12.11 15:06:37 SNTP.CLIENT sent Version 1 SNTP time request to 63.97.45.57
2002.12.11 15:06:37 SNTP.CLIENT received SNTP reply packet from 63.97.45.57
2002.12.11 15:06:37 SNTP.CLIENT setting time to 12-11-2002 15:06:02 UTC
2002.12.11 15:06:37 SNTP.CLIENT waiting for 86400 seconds for the next poll interval
```

debug spanning-tree bpdu [receive | transmit | all]

Use the **debug spanning-tree bpdu** command to display bridge protocol data unit (BPDU) debug messages. When enabled, a debug message is displayed for each BPDU packet that is transmitted or received by the unit. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

receive	Displays debug messages for BPDU packets received by the unit.
transmit	Displays debug messages for BPDU packets transmitted by the unit.
all	Displays debug messages for BPDU packets that are transmitted and received by the unit.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example displays debug messages for BPDU packets that are transmitted and received by the unit:

```
>enable
#debug spanning-tree bpdu all
```

debug spanning-tree [config | events | general | root]

Use the **debug spanning-tree** command to enable the display of spanning-tree debug messages. Debug messages are displayed (real time) on the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

config	Enables the display of spanning-tree debug messages when configuration changes occur.
events	Enables the display of debug messages when spanning-tree protocol events occur.
general	Enables the display of general spanning-tree debug messages.
root	Enables the display of debug messages related to the spanning-tree root.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables the display of general spanning-tree debug messages:

```
>enable
#debug spanning-tree general
```

debug system

Use the **debug system** command to enable debug messages associated with system events (i.e., login, logouts, etc.). Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with system information:

```
>enable
#debug system
```

debug tacacs+ packets

Use the **debug tacas+ packets** command to activate debug messages associated with terminal access controller access control system (TACACS+) protocol. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

No subcommands.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated with the TACACS+ protocol:

```
>enable
#debug tacacs+ packets
```

debug tftp [client | server] packets

Use the **debug tftp packets** command to activate debug messages associated with Trivial File Transfer Protocol (TFTP) packets. Debug messages are displayed (real time) to the terminal (or Telnet) screen. Use the **no** form of this command to disable the debug messages.

Syntax Description

client	Activates TFTP client packet debug messages.
server	Activates TFTP server packet debug messages.

Default Values

By default, all debug messages in the AOS are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example activates debug messages associated TFTP server packets:

```
>enable
#debug tftp server packets
```

dir

Use the **dir** command to display a directory list of files on the system.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is sample output from the **dir** command:

```
>enable
#dir
Files:
 988161 NV3200A-02-00-11.biz
   1152 startup-config
   1113 startup-config.bak
1739729 030018adv.biz
 231424 boot030015.biz
1352150 NV3200A-E03-00-17.biz
 232894 boot030018.biz
1812281 NV3200A-E03-00-20-adv.biz
6366976 bytes used, 335104 available, 6702080 total
```

dir [*<input>* | flash | flash *<input>*]

Use the **dir flash** command to list all of the files stored in flash.

Syntax Description

<input>	Lists all files stored in flash that match the specified pattern.
flash	Lists all files stored in flash.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following is example lists all files stored in flash:

```
>enable
#dir flash
```

disable

Use the **disable** command to exit the Enable mode and enter the Basic mode.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example exits the Enable mode and enters the Basic Command mode:

```
#disable
>
```

enable

Use the **enable** command to enter a password for the Enable mode.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Functional Notes

The Enable Command mode provides access to operating and configuration parameters and should be password protected to prevent unauthorized use. Use the **enable password** command (found in the Global Configuration mode) to specify an Enable Command mode password. If the password is set, access to the Enable Commands (and all other "privileged" commands) is only granted when the correct password is entered. Refer to *enable password [md5] <password>* on page 335 for more information.

Usage Examples

The following example enters the Enable Command mode and defines an Enable Command mode password:

```
>enable
Password: *****
#
```

erase [*<filename>* | startup-config]

Use the **erase** command to erase the specified file.

Syntax Description

<filename>	Specifies the name of the file (located in FLASH memory) to erase.
startup-config	Erases the startup configuration file stored in NVRAM.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example erases the startup configuration file stored in NVRAM:

```
>enable
#erase startup-config
```

If a new startup-configuration file is not specified before power-cycling the unit, the AOS will initialize using a default configuration.

events

Use the **events** command to enable event reporting to the current command line interface (CLI) session. Use the **no** form of this command to disable all event reporting to the current CLI session.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example enables event reporting:

```
>enable
#events
```

exception report generate

Use the **exception report generate** command to immediately generate an exception report.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example immediately generates an exception report:

```
>enable
#exception report generate
```

logout

Use the **logout** command to terminate the current session and return to the login screen.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example shows the logout command being executed in Enable mode:

```
>enable
#logout

Session now available
Press RETURN to get started.
```

ping *<address>*

Use the **ping** command (at the Enable mode prompt) to verify IP network connectivity.

Syntax Description

<address>	Optional. Specifies the IP address of the system to ping. Entering the **ping** command with no specified address prompts the user with parameters for a more detailed **ping** configuration. Refer to *Functional Notes* (below) for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **ping** command helps diagnose basic IP network connectivity using the Packet Internet Groper program to repeatedly bounce Internet Control Message Protocol (ICMP) Echo_Request packets off a system (using a specified IP address). The AOS allows executing a standard **ping** request to a specified IP address or provides a set of prompts to configure a more specific **ping** configuration.

The following is a list of output messages from the **ping** command:

!	Success
-	Destination Host Unreachable
$	Invalid Host Address
X	TTL Expired in Transit
?	Unknown Host
*	Request Timed Out

The following is a list of available extended **ping** fields with descriptions:

Target IP address: Specifies the IP address of the system to ping.

Repeat Count: Specifies the number of ping packets to send to the system (valid range: 1 to 1,000,000).

Datagram Size: Size (in bytes) of the ping packet (valid range: 1 to 1448).

Timeout in Seconds: If a ping response is not received within the timeout period, the ping is considered unsuccessful (valid range: 1 to 5 seconds).

Extended Commands: Specifies whether additional commands are desired for more ping configuration parameters.

Source Address: Specifies the IP address to use as the source address in the ECHO_REQ (or interface) packets.

Data Pattern: Specifies an alphanumerical string to use (the ASCII equivalent) as the data pattern in the ECHO_REQ packets.

Sweep Range of Sizes: Varies the sizes of the ECHO_REQ packets transmitted.

Sweep Min Size: Specifies the minimum size of the ECHO_REQ packet (valid range: 0 to 1488).

Sweep Max Size: Specifies the maximum size of the ECHO_REQ packet (valid range: Sweep Min Size to 1448).

Sweep Interval: Specifies the interval used to determine packet size when performing the sweep (valid range: 1 to 1448).

Verbose Output: Specifies an extended results output.

Usage Examples

The following is an example of a successful **ping** command:

```
>enable
#ping
Target IP address:192.168.0.30
Repeat count[1-1000000]:5
Datagram Size [1-1000000]:100
Timeout in seconds [1-5]:2
Extended Commands? [y or n]:n
Type CTRL+C to abort.
Legend: '!' = Success '?' = Unknown host '$' = Invalid host address
        '*' = Request timed out '-' = Destination host unreachable
        'x' = TTL expired in transit

Pinging 192.168.0.30 with 100 bytes of data:
!!!!!
Success rate is 100 percent (5/5) round-trip min/avg/max = 19/20.8/25 ms
```

reload [cancel | in <*delay*>]

Use the **reload** command to preform a manual reload of the AOS.

> CAUTION *Performing an AOS **reload** disrupts data traffic.*

Syntax Description

cancel Optional. Deactivates a pending **reload** command.

in Optional. Specifies a delay period the AOS will wait before reloading.

<*delay*> Specifies the delay period in minutes (mmm) or hours and minutes (hh:mm).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1 Command was introduced.

Usage Examples

The following example reloads the AOS software in 3 hours and 27 minutes:

```
>enable
#reload in 03:27
```

The following example reloads the AOS software in 15 minutes:

```
>enable
#reload in 15
```

The following example terminates a pending reload command:

```
>enable
#reload cancel
```

show access-lists *<listname>*

Use the **show access-lists** command to display all configured access lists in the system (or a specific list).

Syntax Description

<listname>	Optional. Specifies a particular access list to display.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The **show access-lists** command displays all configured access lists in the system. All entries in the access list are displayed, and a counter indicating the number of packets matching the entry is listed.

Usage Examples

The following is a sample output from the **show access-lists** command:

```
>enable
#show access-lists

Standard access list MatchAll
permit host 10.3.50.6 (0 matches)
permit 10.200.5.0 wildcard bits 0.0.0.255 (0 matches)
extended access list UnTrusted
deny icmp 10.5.60.0 wildcard bits 0.0.0.255 any source-quench (0 matches)
deny tcp any (0 matches)
```

show arp [realtime]

Use the **show arp** command to display the Address Resolution Protocol (ARP) table.

Syntax Description

realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample output of the **show arp** command:

```
>enable
#show arp

ADDRESS           TTL (min)   MAC ADDRESS         LAST UPDATED (min)   INTERFACE
192.168.30.36     13          00:E0:7D:88:1A:B9   4260                 eth 0/1
192.168.30.253    17          02:60:8C:DD:0A:CE   4264                 eth 0/1
224.0.0.9         71578541    01:00:5E:00:00:09   0                    eth 0/2
```

show auto-config

Use the **show auto-config** command to display auto-configuration status.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following is a sample output of the **show auto-config** command:

```
>enable
#show auto-config
Auto-Config is enabled, current status: Done.
 TFTP Server is 10.20.20.1
 Config filename is 1524STfile
        Maximum retry count is 0 (repeat indefinitely), total retries is 0
```

show bridge *<interface> <slot/port> <bridge group #>*

Use the **show bridge** command to display a list of all configured bridge groups (including individual members of each group). Enter an interface or a bridge number to display the corresponding list.

Syntax Description

<interface> <slot/port>	Optional. Displays all bridge groups associated with the specific interface. Type the **show bridge ?** command to display a list of applicable interfaces.
<bridgegroup#>	Optional. Displays a specific bridge group

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC interface.

Usage Examples

The following is a sample output from the **show bridge** command:

```
>enable
#show bridge

Total of 300 station blocks 295 free
Address              Action     Interface    Age     Rx Count    Tx Count
00:04:51:57:4D:5A    forward    eth 0/1      0       7133392     7042770
00:04:5A:57:4F:2A    forward    eth 0/1      0       402365      311642
00:10:A4:B3:A2:72    forward    eth 0/1      4       2           0
00:A0:C8:00:8F:98    forward    eth 0/1      0       412367      231
00:E0:81:10:FF:CE    forward    fr 1.17      0       1502106     1486963
```

show buffers [realtime]

Use the **show buffers** command to display the statistics for the buffer pools on the network server.

Syntax Description

realtime — Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample output from the **show buffers** command:

```
>enable
#show buffers
Buffer handles: 119 of 2000 used.

Pool   Size     Total   Used   Available   Max. Used
0      1800     1894    119    1775        122
1      2048     64      0      64          0
2      4096     32      0      32          0
3      8192     4       0      4           0
4      16384    2       0      2           0
5      32768    2       0      2           0
```

show buffers users [realtime]

Use the **show buffers users** command to display a list of the top users of packet buffers. Typically, this command will only be used as a debug tool by ADTRAN personnel.

Syntax Description

realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample from the **show buffers users** command:

```
>enable
#show buffers users
Number of users: 7
Rank        User              Count
  1         0x0052f4f8        59
  2         0x0051a4fc        32
  3         0x00528564        8
  4         0x0053c1c8        7
  5         fixedsize         5
  6          0x001d8298          2
  7          0x0010d970          1
  8          0x00000000          0
  9          0x00000000          0
 10          0x00000000          0
 11          0x00000000          0
 12          0x00000000          0
 13          0x00000000          0
 14          0x00000000          0
 15          0x00000000          0
```

show clock [detail]

Use the **show clock** command to display the system time and date entered using the **clock set** command. Refer to the section *clock set <time> <day> <month> <year>* on page 78 for more information.

Syntax Description

detail	Optional. Displays more detailed clock information, including the time source.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays the current time and data from the system clock:

```
>show clock

23:35:07 UTC Tue Aug 20 2002
```

show configuration

Use the **show configuration** command to display a text printout of the startup configuration file stored in nonvolatile random access memory (NVRAM).

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample output of the **show configuration** command:

```
>enable
#show configuration
!
!
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
logging forwarding priority-level info
no logging email
!
ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
!
```

```
!
!
interface eth 0/1
speed auto
  no ip address
  shutdown
!
interface dds 1/1
  shutdown
!
interface bri 1/2
  shutdown
!
!
ip access-list standard Outbound
  permit host 10.3.50.6
  permit 10.200.5.0 0.0.0.255
!
!
ip access-list extended UnTrusted
  deny   icmp 10.5.60.0 0.0.0.255 any source-quench
  deny   tcp any any
!
no ip snmp agent
!
!
!
line con 0
  no login
!
line telnet 0
  login
line telnet 1
  login
line telnet 2
  login
line telnet 3
  login
line telnet 4
  login
!
```

show connections

Use the **show connections** command to display information (including TDM group assignments) for all active connections.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following is sample output from the **show connections** command:

```
>enable
#show connections

Displaying all connections....
Conn ID
From
To
1
ppp 1
e1 1/1, tdm-group 1
```

show crypto ca [certificates | crls | profiles]

Use the **show crypto ca** command to display information regarding certificates and profiles.

Syntax Description

certificates	Displays information on all certificates.
crls	Displays a summary of all certificate revocation lists (CRLs) for each CA.
profiles	Displays information on all configured CA profiles.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced (enhanced software version only).

Usage Examples

The following is a sample from the **show crypto ca certificates** command:

```
>enable
#show crypto ca certificates
CA Certificate
 Status: Available
 Certificate Serial Number: 012d
 Subject Name: /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1
 Issuer: /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1
 CRL Dist. Pt: /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1
 Start date is Jan 9 16:25:15 2003 GMT
 End date is Dec 31 23:59:59 2003 GMT
 Key Usage:
   Non-Repudiation
   Key Encipherment
   Data Encipherment
   CRL Signature
   Encipherment Only
```

show crypto ike

Use the **show crypto ike** command to display information regarding the IKE configuration.

Variations of this command include the following:

show crypto ike client configuration pool
show crypto ike client configuration pool *<poolname>*
show crypto ike policy
show crypto ike policy *<policy priority>*
show crypto ike remote-id *<remote-id>*
show crypto ike sa

Syntax Description

client configuration pool	Displays the list of all configured IKE client configuration pools.
<poolname>	Displays detailed information regarding the specified IKE client configuration pool.
policy	Displays information on all IKE policies. Indicates if client configuration is enabled for the IKE policies and displays the pool names.
<policy priority>	Displays detailed information on the specified IKE policy. This number is assigned using the **crypto ike policy** command. Refer to *crypto ike* on page 322 for more information.
remote-id *<remote-id>*	Displays information on all IKE information regarding the remote-id. The remote-id value is specified using the **crypto ike remote-id** command (refer to *crypto ike remote-id* on page 326).
sa	Displays the configuration of active IKE security associations.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following is a sample from the **show crypto ike policy** command:

```
>enable
#show crypto ike policy
Crypto IKE Policy 100
  Main mode
  Using System Local ID Address
  Peers:
  63.105.15.129
initiate main
respond anymode
  Attributes:
    10
      Encryption: 3DES
      Hash: SHA
      Authentication: Pre-share
      Group: 1
      Lifetime: 900 seconds
```

show crypto ipsec

Use the **show crypto ipsec** command to display information regarding the IPSec configuration.

Variations of this command include the following:

show crypto ipsec sa
show crypto ipsec sa address <*ip address*>
show crypto ipsec sa map <*mapname*>
show crypto ipsec transform-set
show crypto ipsec transform-set <*transform-set name*>

Syntax Description

sa	Displays all IPSec security associations.
sa address <*ip address*>	Displays all IPSec security associations associated with the designated peer IP address.
sa map <*mapname*>	Displays all IPSec security associations associated with the designated crypto map name.
transform-set	Displays all defined transform sets.
<*transform-set name*>	Displays information for a specific transform set.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

show crypto map

Use the **show crypto map** command to display information regarding crypto map settings.

Variations of this command include the following:

show crypto map

show crypto map <*interface*>

show crypto map <*map name*>

show crypto map <*map name*> <*map number*>

Syntax Description

<*interface*>	Displays the crypto map settings for the specified interface. Type **show interfaces ?** for a complete list of valid interfaces.
<*map name*>	Specifies a specific crypto map name.
<*map number*>	Specifies a specific crypto map number.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following is a sample from the **show crypto map** command:

```
> enable
#show crypto map testMap

Crypto Map "testMap" 10 ipsec-ike
  Extended IP access list NewList
  Peers:
    63.97.45.57
  Transform sets:
    esp-des
  Security-association lifetimes:
    0 kilobytes
    86400 seconds
  No PFS group configured
  Interfaces using crypto map testMap:
    eth 0/1
```

show debugging

Use the **show debugging** command to display a list of all activated debug message categories.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample output from the **show debugging** command:

```
>enable
#show debugging

debug access-list MatchAll
debug firewall
debug ip rip
debug frame-relay events
debug frame-relay llc2
debug frame-relay lmi
```

show demand

Use the **show demand** command to display information regarding demand routing parameters and statistics.

Variations of this command include the following:

show demand
show demand interface
show demand interface <*interface*>
show demand resource pool
show demand resource pool <*resource pool name*>
show demand sessions

Syntax Description

interface	Displays the information for all demand routing interfaces.
interface <*interface*>	Displays information for a specific demand routing interface. Valid range: 1 to 1024. Type **show demand interface ?** for a list of valid interfaces.
resource pool	Displays all resource pool information.
resource pool <*resource pool name*>	Displays resource pool information for a specific resource pool name.
sessions	Displays active demand sessions.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following is example output from the **show demand interface** command:

```
>enable
#show demand int 1
Demand 1 is UP (connected)
  Configuration:
```

```
  Keep-alive is set (10 sec.)
  Admin MTU = 1500
  Mode: Either, 1 dial entries, idleTime = 120, fastIdle = 20
  Resource pool demand
  No authentication configured
  IP address 10.100.0.2 255.255.255.0
 Connect Sequence: Successes = 0, Failures = 0
  Seq    DialString   Technology  Successes Busys NoAnswers NoAuths InUse
    5      5552222        ISDN       0      0         0       0
 Current values:
  Local IP address 10.100.0.2, Peer IP address 10.100.0.1
  Seconds until disconnect: 63
  Queueing method: weighted fair
  Output queue: 0/1/428/64/0 (size/highest/max total/threshold/drops)
    Conversations  0/1/256 (active/max active/max total)
    Available Bandwidth 48 kilobits/sec
  Bandwidth=64 Kbps
 Link through bri 1/3, Uptime 0:01:10
  IN: Octets 588, Frames 19, Errors 0
  OUT: Octets 498, Frames 18, Errors 0
  Last callerID 2565552222, last called num 5552222
```

The following is example output from the **show demand interface demand** command:

```
>enable
#show demand interface demand 1
demand 1
Idle timer (120 secs), Fast idle timer (20 secs)

Dialer state is data link layer up
Dial reason: answered

Interface bound to resource bri 1/3
Time until disconnect 105 secs
Current call connected 00:00:27
Connected to 2565552222

Number of active calls = 1
Interesting Traffic = list junk

 Connect Sequence: Successes = 0, Failures = 0
  Seq    DialString   Technology  Successes Busys NoAnswers NoAuths InUse
    5      5552222        ISDN       0      0         0       0
```

The following is example output from the **show demand resource pool** command:

```
>enable
#show demand resource pool
Pool demand
          Resources:             bri 1/3, bri 2/3
          Demand Interfaces:     demand 1
```

The following is example output from the **show demand sessions** command:

```
>enable
#show demand sessions
Session 1
Interface demand 1
Local IP address = 10.100.0.2
Remote IP address = 10.100.0.1
Remote Username =
Dial reason: ip (s=, d=)
Link 1
  Dialed number = 5552222
  Resource interface = bri 1/3, Multilink not negotiated
  Connect time: 0:0:13
  Idle Timer: 119
```

show dial-backup interfaces

Use the **show dial-backup interfaces** command to display all configured dial-backup interfaces and the associated parameters for each.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include PPP dial backup.

Usage Examples

The following example enters the Enable mode and uses the show command to display dial-backup interface information:

```
>enable
#show dial-backup interfaces
Dial-backup interfaces...
fr 1.16 backup interface:
  Backup state:     idle
  Backup protocol:  PPP
 Call mode:        originate
  Auto-backup:      enabled
  Auto-restore:     enabled
  Priority:         50
  Backup delay:     10 seconds
  Restore delay:    10 seconds
  Connect timeout: 60 seconds

 Redial retries:   unlimited
  Redial delay:     10 seconds
Backup enabled all day on the following days:
     Sunday Monday Tuesday Wednesday Thursday Friday Saturday
```

```
Backup phone number list:
   Number            Call Type   min/max DS0s   Backup I/F
   5551212             analog       1/1           ppp 2
```

show dynamic-dns

Use the **show dynamic-dns** command to show information related to the dynamic domain naming system (DNS) configuration.

Syntax Description

No subcommands.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following is sample output from this command:

```
>enable
#show dynamic-dns
eth 0/1:
 Hostname: host
 Is Updated: no
 Last Registered IP: 10.15.221.33
 Last Update Time: 00:00:00 UTC Thu Jan 01 1970
```

show event-history

Use the **show event-history** command to display all entries in the current local event-history log.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The event history provides useful information regarding the status of the system and individual port states. Use the event history as a troubleshooting tool when identifying system issues. The following is a sample event-history log.

```
>enable
#show event-history

Using 526 bytes
2002.07.12 15:34:01 T1.t1 1/1 Yellow
2002.07.12 15:34:01 INTERFACE_STATUS.t1 1/1 changed state to down.
2002.07.12 15:34:02 T1.t1 1/1 No Alarms
2002.07.12 15:34:02 INTERFACE_STATUS.t1 1/1 changed state to up.
2002.07.12 15:34:03 INTERFACE_STATUS.eth 0/1 changed state to up.
2002.07.12 15:34:10 OPERATING_SYSTEM Warm Start
2002.07.12 15:34:12 PPP.NEGOTIATION LCP up
2002.07.12 15:34:12 PPP.NEGOTIATION IPCP up
```

show fan-tach

Use the **show fan-tach** command to view the unit’s current fan speed.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example shows the current fan speed:

```
>enable
#show fan-tach
 Fan Tach (in rpm)   Current    Min       Max       Avg
 -------------------------------------------------------
 Processor           8160       8100      17804     8544
 Chassis 1           3060       3060      31380     4237
 Chassis 2           3120       3060      31560     4277
```

show flash

Use the **show flash** command to display a list of all files currently stored in FLASH memory.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample **show flash** output:

```
>enable
#show flash

Files:
 245669 010100boot.biz
1141553 new.biz
    821 startup-config
   1638 startup-config.old
1175679 020016.biz
    821 startup-config.bak
2572304 bytes used 4129776 available 6702080 total
```

show frame-relay fragment [frame-relay *<port.sublink>*]

Use the **show frame-relay fragment** command to display FRF.12 statistics for Frame Relay sublinks enabling FRF.12 fragmentation.

Syntax Description

frame-relay *<port.sublink>*	Optional. Displays detailed FRF.12 statistics for the specified Frame Relay sublink (if FRF.12 is enabled on that sublink).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following are sample outputs from various **show frame-relay fragment** commands:

```
>enable
#show frame-relay fragment
interface     dlci      frag_size     rx_frag       tx_frag          dropped_frag
fr 1.1        17        100           46            48               0
fr 1.2        18        200           42            21               0
```

```
>enable
#show frame-relay fragment frame-relay 1.1
DLCI =   17 FRAGMENT SIZE = 100
rx frag. pkts                  46    tx frag. pkts                48
rx frag. bytes               4598    tx frag. bytes             4724
rx non-frag. pkts              18    tx non-frag. pkts            28
rx non-frag. bytes           1228    tx non-frag. bytes         1960
rx assembled pkts              23    tx pre-fragment pkts         34
rx assembled bytes           5478    tx pre-fragment bytes      6324
dropped reassembling pkts       0    dropped fragmenting pkts      0
rx out-of-sequence fragments        0
rx unexpected beginning fragment       0
```

show frame-relay

Use the **show frame-relay** command to display configuration and status parameters for configured virtual Frame Relay interfaces.

Variations of this command include the following:

show frame-relay lmi
show frame-relay pvc
show frame-relay pvc interface frame-relay *<interface>*
show frame-relay pvc realtime

Syntax Description

lmi	Displays Link Management Interface (LMI) statistics for each virtual Frame Relay interface.
pvc	Displays Permanent Virtual Circuit (PVC) configuration and statistics for all virtual Frame Relay interfaces (or a specified interface).
frame-relay	Optional. Displays Frame Relay PVC statistics for a specific Frame Relay interface.
<interface>	Specifies the virtual Frame Relay interface (for example fr 1).
realtime	Displays full-screen output in realtime. See the **Functional Notes** below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 10.1	**Realtime** option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following are sample outputs from various **show frame-relay** commands:

```
>enable
#show frame-relay lmi

LMI statistics for interface FR 1 LMI TYPE = ANSI
Num Status Enq. Sent 79       Num Status Msgs Rcvd 71
Num Update Status Rcvd 12     Num Status Timeouts 5
```

```
>enable
#show frame-relay pvc

Frame Relay Virtual Circuit Statistics for interface FR 1
           Active          Inactive        Deleted         Static
local      2               0               0               2
DLCI = 16 DLCI USAGE = LOCAL PVC STATUS = ACTIVE INTERFACE = FR 1.16
MTU: 1500
input pkts: 355            output pkts: 529                in bytes: 23013
out bytes: 115399          dropped pkts: 13                in FECN pkts: 0
in BECN pkts: 0            in DE pkts: 0                   out DE pkts: 0
pvc create time: 00:00:00:12               last time pvc status changed: 00:00:13:18
DLCI = 20 DLCI USAGE = LOCAL PVC STATUS = ACTIVE INTERFACE = FR 1.20
MTU: 1500
input pkts: 0              output pkts: 44                 in bytes: 0
out bytes: 22384           dropped pkts: 11                in FECN pkts: 0
in BECN pkts: 0            in DE pkts: 0                   out DE pkts: 0
pvc create time: 00:00:01:25               last time pvc status changed: 00:00:13:18
```

show frame-relay multilink *<interface>* detailed

Use the **show frame-relay multilink** command to display information associated with the Frame Relay multilink interface.

Syntax Description

<interface>	Optional. Specifies the display of information for a specific interface. Enter the **show frame-relay multilink ?** command for a complete list of interfaces.
detailed	Optional. Displays more detailed information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following is a sample output from this command:

```
>enable
#show frame-relay multilink
Bundle: frame-relay 1 is DOWN; class A bundle
Near-end BID: MFR1; Far-end BID: unknown
```

show hosts [verbose]

Use the **show hosts** command to display information such as the domain name, name lookup service, a list of name server hosts, and the cached list of host names and addresses on the network to which you can connect.

Syntax Description

verbose	Enables detailed messaging.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1

Functional Notes

The list below describes the fields contained in the host table:

- Flags: Indicate whether the entry is permanent (P) or temporary (T) and if the entry is OK or expired (EXP).
- Age: Indicates the age of the entry.
- Type: Shows the protocol type.
- Address: Displays the IP address for the entry.

Usage Examples

The following example is sample output from the **show hosts** command:

```
>enable
#show hosts

Name/address lookup uses domain name service
DNS Proxy is disabled
Default domain is not set
Name servers are 1.1.1.1 2.2.2.2
Host          Flags      Age     Type     Address
Example1      (P OK)     - -     IP       1.1.1.1
Example2      (P OK)     - -     IP       2.2.2.2
```

show interfaces *<interface>*

Use the **show interfaces** command to display configuration parameters and current statistics for all interfaces (or a specified interface).

Syntax Description

<interface> Optional. Specifies the interface to display. Type **show interfaces ?** for a complete list of valid interfaces.

description Optional. Displays information such as name, administrative status, protocol, and description for all the interfaces.

performance-statistics Optional. Displays the current 15-minute interval, the current 24-hour totals, and all 96 stored intervals.

performance-statistics total-24-hour Optional. Displays the current 24-hour totals and the past seven 24-hour intervals.

performance-statistics *<x-y>* Shows the current 15-minute interval, the current 24-hour totals, and all intervals from x through y. This command is basically the same thing as the **performance-statistics** command with the added function of allowing you to specify a particular interval (or range of intervals) to display rather than displaying all 96.

> *Note: If you want to display the 24th interval, enter (for example)* ***show interface t11/1 performance-statistics 24-24****. Entering* ***show interface t1 1/1 performance-statistics 24*** *results in displaying the 24-hour statistics. Any number other than 24 (between 1 and 96) results in the correct display of the selected interval (e.g.,* ***show interface t1 1/1 performance-statistics 4*** *shows the fourth interval).*

realtime Displays full-screen output in real time. See the *Functional Notes* below for more information.

status Optional. Displays information such as name, type, status, VLAN, speed, and duplex for all the Ethernet interfaces only.

verbose Displays detailed configuration information on the terminal screen (versus only the non-default values).

version Optional. Displays current version information (e.g., model and list number, software version, etc.) for the T1 interface.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 6.1	Command was updated to include performance-statistics option.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.
Release 10.1	The realtime option and PRI interface were added.
Release 11.1	Description, status, and verbose options were introduced. The demand, FXO, and serial interfaces were added.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following are samples from various **show interfaces** commands:

```
>enable
#show interfaces t1 1/1

t1 1/1 is UP
  T1 coding is B8ZS framing is ESF
  Clock source is line FDL type is ANSI
  Line build-out is 0dB
  No remote loopbacks No network loopbacks

  DS0 Status: 123456789012345678901234
              NNNNNNNNNNNNNNNNNNNNNNNN

  Line Status: -- No Alarms --

  Current Performance Statistics:
    0 Errored Seconds 0 Bursty Errored Seconds
    0 Severely Errored Seconds 0 Severely Errored Frame Seconds
    0 Unavailable Seconds 0 Path Code Violations
    0 Line Code Violations 0 Controlled Slip Seconds
    0 Line Errored Seconds 0 Degraded Minutes
```

```
#show interfaces modem 1/2
modem 1/2 is UP
  Line status: on-hook
  Caller ID will be used to route incoming calls
    0 packets input 0 bytes 0 no buffer
    0 runts 0 giants 0 throttles
    0 input errors 0 CRC 0 frame
    0 abort 0 ignored 0 overruns
    0 packets output 0 bytes 0 underruns
    0 input clock glitches 0 output clock glitches
    0 carrier lost 0 cts lost
```

```
#show interfaces eth 0/1
Ip address is 10.200.1.50
  Netmask is 255.255.0.0
  MTU is 1500
  Fastcaching is Enabled
  RIP Authentication is Disabled
  RIP Tx uses global version value
  RIP Rx uses global version value
```

```
#show interfaces dds 1/1
dds 1/1 is UP line protocol is UP
  Encapsulation FRAME-RELAY (fr 1)
  Loop rate is set to 56000 actual rate is 56000
  Clock source is line
  Data scrambling is disabled
  No Loopbacks
    75 packets input 6108 bytes 0 no buffer
    0 runts 0 giants 0 throttles
    0 input errors 0 CRC 0 frame
    0 abort 0 ignored 0 overruns
    81 packets output 11496 bytes 0 underruns
    0 input clock glitches 0 output clock glitches
    0 carrier lost 0 cts lost
```

```
#show interfaces fr 1
TDM group 10 line protocol is UP
Encapsulation FRAME-RELAY (fr 1)
  463 packets input 25488 bytes 0 no buffer
  0 runts 0 giants 0 throttles
  0 input errors 0 CRC 0 frame
  0 abort 0 ignored 0 overruns
  864 packets output 239993 bytes 0 underruns
  0 input clock glitches 0 output clock glitches
  0 carrier lost 0 cts lost

 Line Status: -- No Alarms --

 Current Performance Statistics:
  0 Errored Seconds 0 Bursty Errored Seconds
  0 Severely Errored Seconds 0 Severely Errored Frame Seconds
  0 Unavailable Seconds 0 Path Code Violations
  0 Line Code Violations 0 Controlled Slip Seconds
  0 Line Errored Seconds 0 Degraded Minutes
```

```
#show interfaces fr 1.100*
fr 1.100 is Active
Ip address is 63.97.45.57, mask is 255.255.255.248
Interface-dlci is 100
MTU is 1500 bytes, BW is 96000 Kbit (limited)
Average utilization is 53%
```

*Note: If the user has configured a **Bc** and **Be** value on the virtual circuit, the bandwidth (**BW**) displayed is the sum of those values (Bc + Be). If not, the value for **BW** is the speed of the interface. The **Average utilization** displayed is the average utilization of the displayed bandwidth. If the bandwidth number is the Bc + Be value, the **(limited)** text appears (as shown above).

show ip access-lists *<listname>*

Use the **show ip access-lists** command to display all configured IP access lists in the system.

Syntax Description

<listname>	Optional. Specifies a particular access list to display.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The **show ip access-lists** command displays all configured IP access lists in the system. All entries in the access list are displayed, and a counter indicating the number of packets matching the entry is listed.

Usage Examples

The following is a sample output from the **show ip access-lists** command:

```
>enable
#show ip access-lists

Standard IP access list MatchAll
   permit host 10.3.50.6 (0 matches)
   permit 10.200.5.0 wildcard bits 0.0.0.255 (0 matches)
Extended IP access list UnTrusted
   deny   icmp 10.5.60.0 wildcard bits 0.0.0.255 any source-quench (0 matches)
   deny   tcp any any   (0 matches)
```

show ip arp [realtime]

Use the **show ip arp** command to display the Address Resolution Protocol (ARP) table.

Syntax Description

realtime	Displays full-screen output in realtime. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample output of the **show ip arp** command:

```
>enable
#show ip arp

ADDRESS            TTL (min)     MAC ADDRESS          LAST UPDATED (min)
192.168.30.36      13            00:E0:7D:88:1A:B9    4260
192.168.30.253     17            02:60:8C:DD:0A:CE    4264
224.0.0.9          71578541      01:00:5E:00:00:09    0
```

show ip as-path-list [*<listname>*]

Use the **show ip as-path-list** command to display any AS path lists that have been configured in the router, along with any permit and deny clauses in each list.

Syntax Description

<listname> Optional. Specifies that the command display only the list matching the specified AS path listname. If not specified, all AS path lists are displayed.

Default Values

By default, this command displays all AS path lists.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 10.1 Command was introduced.

Usage Examples

In the following example, all AS path lists defined in the router are displayed.

```
>enable
#show ip as-path-list
ip as-path-list AsPathList1:
  permit 100
  permit 200
  permit 300
  deny 6500
ip as-path-list AsPathList2:
  permit 400
  permit 500
```

In the following example, only the AS Path List with the name **AsPathList2** is displayed.

```
>enable
#show ip as-path-list AsPathList2
ip as-path-list AsPathList2:
  permit 400
  permit 500
```

show ip bgp community [*<community number> . . . <community number>* | internet | no export| local-as | no-advertise] [exact]

Use the **show ip bgp community** command to display only those routes learned via Border Gateway Protocol (BGP) that match the community numbers specified in the command. If no communities are specified, all BGP routes are shown.

Syntax Description

<community-number>	Optional. Displays routes that contain this value in their community attribute. This is a numeric value that can be an integer from 1 to 4,294,967,295 or string in the form “aa:nn", where the value of "aa" is the AS number and the value of "nn" is the community number. Multiple community-number parameters can be present in the command.
internet	Optional. Displays routes that contain this value in their community attribute. This represents the well-known reserved community number for the INTERNET community.
local-as	Optional. Displays routes that contain this value in their community attribute. This represents the well-known reserved community number for NO_EXPORT_SUBCONFED. Routes containing this attribute should not be advertised to external BGP peers.
no-export	Optional. Displays routes containing this value in the community attribute. This represents the well-known reserved community number for NO_EXPORT. Routes containing this attribute should not be advertised to BGP peers outside a confederation boundary.
no-advertise	Optional. Displays routes containing this value in the community attribute. This represents the well-known reserved community number for NO_ADVERTISE. Routes containing this attribute should not be advertised to any BGP peer.
exact	Optional. Displays BGP routes with the community numbers specified and *only* those specified.

Default Values

By default, this command displays all BGP routes.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

In the following example, all BGP routes are displayed whose community numbers match those listed in the **show ip bgp community** command.

```
>enable
#show ip bgp community local-as 10:405
BGP local router ID is 10.22.131.241, local AS is 302.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop        Metric     LocPrf       Path
        10.22.152.20/30  10.22.131.10    304                     302 300 1 3 4 i
        10.22.152.24/29  10.22.131.10    304                     302 300 1 3 4 5 i
        10.22.152.36/30  10.22.131.10    304                     302 300 1 3 4 i
        10.22.152.52/30  10.22.131.10    304                     302 300 1 3 4 i
        11.0.0.0/30      10.22.131.10    304                     302 300 1 3 4 6 i
        12.0.0.0/30      10.22.131.10    304                     302 300 1 3 4 6 i
        13.0.0.0/30      10.22.131.10    304                     302 300 1 3 4 6 i
        14.0.0.0/30      10.22.131.10    304                     302 300 1 3 4 6 i
        20.0.0.0/30      10.22.131.10    304                     302 300 1 3 4 5 i
        21.0.0.0/30      10.22.131.10    304                     302 300 1 3 4 5 i
Total RIB entries = 10
```

Information displayed includes: the ID of this router and its Autonomous System (AS) number; the destination Network address of the route learned; the Next Hop address to that network; the Metric; the Local Preference value (set using the **set local-preference** command); and the AS Path to the destination network.

The following is a sample output for the show-ip bgp community command with an exact match specified: BGP routes with the community numbers specified and *only* those specified are shown

```
>enable
#show ip bgp community 1001 2001 3001 exact
BGP local router ID is 192.168.9.1, local AS is 252.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete

         Network             NextHop         Metric    LocPrf        Path
         *  192.168.11.0/24  10.22.27.251                            249 251 i
         *  192.168.12.0/24  10.22.27.251                            249 251 i
         *> 192.168.32.0/24  10.22.27.249                            249 i
         *> 192.168.33.0/24  10.22.27.249                            249 i
Total RIB entries = 4
```

show ip bgp community-list *<community-list-name>* [exact]

Use the **show ip bgp community-list** command to display Border Gateway Protocol (BGP) routes that are permitted by the specified community list.

Syntax Description

<community-list-name>	Specifies the name of the community list whose routes you wish to see.
exact	Optional. Restricts the routes displayed to only those whose community lists exactly match those specified in the named community list. If this parameter is omitted, all routes matching any part of the specified community list will be displayed.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Functional Notes

Information displayed includes the ID of this router and its Autonomous System number, the destination Network address of the route learned, the Next Hop address to that network, the Metric, the Local Preference value (set using the "set local-preference *" command), and the Autonomous System Path to the destination network.

Usage Examples

In the following example, all BGP routes are displayed whose community numbers match those defined in the community list named CList1.

```
>enable
#show ip bgp community-list CList1
BGP local router ID is 10.22.131.241, local AS is 302.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop        Metric     LocPrf        Path
        10.22.152.20/30  10.22.131.10    304                      302 300 1 3 4 i
        10.22.152.24/29  10.22.131.10    304                      302 300 1 3 4 5 i
        10.22.152.36/30  10.22.131.10    304                      302 300 1 3 4 i
        10.22.152.52/30  10.22.131.10    304                      302 300 1 3 4 i
        11.0.0.0/30      10.22.131.10    304                      302 300 1 3 4 6 i
        12.0.0.0/30      10.22.131.10    304                      302 300 1 3 4 6 i
        13.0.0.0/30      10.22.131.10    304                      302 300 1 3 4 6 i
        14.0.0.0/30      10.22.131.10    304                      302 300 1 3 4 6 i
        20.0.0.0/30      10.22.131.10    304                      302 300 1 3 4 5 i
        21.0.0.0/30      10.22.131.10    304                      302 300 1 3 4 5 i
Total RIB entries = 10
```

show ip bgp [regexp *<expression>* | summary]

Use the **show ip bgp** command to display a summary of the Border Gateway Protocol (BGP) route table.

Syntax Description

<expression>	Specifies the regular expression to filter on.
regexp	Displays routes whose autonomous system (AS) path matches the regular expression specified.
summary	Displays a summary of the status for all BGP.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

Entries that are not filtered by prefix lists are marked with an asterisk (*) to show they are valid. Entries that are deemed the best path to advertised route are marked with a caret (>).

Usage Examples

The following sample output of the **show ip bgp** command shows all of the entries in the BGP database.

```
Router#show ip bgp
BGP local router ID is 192.168.3.1, local AS is 304.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network           Next Hop       Metric    LocPrf  Path
*> 10.22.130.8/29    10.22.131.1                      302 i
*> 10.22.130.8/29    10.22.131.9                      302 i
   10.22.130.8/29    10.22.132.9                      303 304 302 i
*> 10.22.130.240/28  10.22.131.1                      302 300 i
*> 10.22.130.240/28  10.22.131.9                      302 300 i
*  i10.22.130.240/28 10.22.132.1              100     303 300 i
*   10.22.130.240/28    10.22.132.9                        303 300 i
*>  10.22.131.0/29      10.22.131.1                        302 i
*>  10.22.131.0/29      10.22.131.9                        302 i
    10.22.131.0/29      10.22.132.9                        303 304 302 i
*>  10.22.131.8/29      10.22.131.1                        302 i
*>  10.22.131.8/29      10.22.131.9                        302 i
    0.22.131.8/29       10.22.132.9                        303 304 302 i
*>  10.22.131.16/29     10.22.131.1                        302 i
*>  10.22.131.16/29     10.22.131.9                        302 i
*   i10.22.131.16/29    10.22.132.1     0          100     303 i
*   10.22.131.16/29     10.22.132.9     0                  303 i
*>  10.22.131.240/28    10.22.131.1                        302 i
*>  10.22.131.240/28    10.22.131.9                        302 i
*   i10.22.131.240/28   10.22.132.1                100     303 300 i
*   10.22.131.240/28    10.22.132.9                        303 300 i
*   10.22.132.0/29      10.22.131.1     0                  302 303 i
*   10.22.132.0/29      10.22.131.9     0                  302 303 i
*   i10.22.132.0/29     10.22.132.1     0          100     303 i
*>  10.22.132.0/29      10.22.132.9     0                  303 i
*>  o10.22.132.8/29     0.0.0.0                            i
*   10.22.132.8/29      10.22.131.1     0                  302 303 i
*   10.22.132.8/29      10.22.131.9     0                  302 303 i
*   10.22.132.8/29      10.22.132.9     0                  303 i
*   10.22.132.240/28    10.22.131.1                        302 300 i
*   10.22.132.240/28    10.22.131.9                        302 300 i
*   i10.22.132.240/28   10.22.132.1     0          100     303 i
*>  10.22.132.240/28    10.22.132.9     0                  303 i
*>  o10.22.134.0/29     0.0.0.0                            i
*   i10.22.134.0/29     10.22.134.1                100     i
    10.22.134.0/29      10.22.131.9                        302 304 i
    10.22.134.0/29      10.22.132.9                        303 304 i
*>  i10.22.134.8/29     10.22.134.10               100     i
    10.22.134.8/29      10.22.131.9                        302 304 i
    10.22.134.8/29      10.22.132.9                        303 304 i
*>  i10.22.134.16/29    10.22.134.1                100     i
*>  i10.22.134.16/29    10.22.134.26               100     i
    10.22.134.16/29     10.22.131.9                        302 304 i
    10.22.134.16/29     10.22.132.9                        303 304 i
*>  o10.22.134.24/29    0.0.0.0                            i
*    i10.22.134.24/29   10.22.134.26               100     i
    10.22.134.24/29     10.22.131.9                        302 304 i
    10.22.134.24/29     10.22.132.9                        303 304 i
*>  o10.22.134.32/29     0.0.0.                            i
*   i10.22.134.32/29    10.22.134.34               100     i
```

```
   10.22.134.32/29  10.22.131.9                    303 304 i
*> i10.22.134.40/29 10.22.134.10           100     i
   10.22.134.40/29  10.22.131.9                    302 304 i
   10.22.134.40/29  10.22.132.9                    303 304 i
*> i10.22.134.48/29 10.22.134.26           100     i
*> i10.22.134.48/29 10.22.134.34           100     i
   10.22.134.48/29  10.22.131.9                    302 304 i
   10.22.134.48/29  10.22.132.9                    303 304 i
*> i10.22.134.56/29 10.22.134.26           100      i
   10.22.134.56/29  10.22.131.9                    302 304 i
   10.22.134.56/29  10.22.132.9                    303 304 i
*> i10.22.134.64/29 10.22.134.26           100     i
*> i10.22.134.64/29 10.22.134.34           100      i
   10.22.134.64/29  10.22.131.9                    302 304 i
   10.22.134.64/29  10.22.132.9                    303 304 i
*> i10.22.134.80/29 10.22.134.26           100     i
   10.22.134.80/29  10.22.131.9                    302 304 i
   10.22.134.80/29  10.22.132.9                    303 304 i
   10.22.135.0/29   10.22.131.9   333              302 304 305 i
   10.22.135.0/29   10.22.132.9                    303 304 305 i
*> i10.22.135.0/29  10.22.134.82  333      100     305 i
   10.22.135.8/29   10.22.131.9   333              302 304 305 i
   10.22.135.8/29   10.22.132.9                    303 304 305 i
*> i10.22.135.8/29  10.22.134.82  333      100     305 i
*> i192.168.1.0/24  10.22.134.1            100     i
*> i192.168.2.0/24  10.22.134.26           100     i
*> o192.168.3.0/24   0.0.0.0                       i
*> i192.168.4.0/24  10.22.134.34           100     i
*> i192.168.6.0/24  10.22.134.82  333      100     305 i
Total RIB entries = 80
```

The following sample output of the **show ip bgp summary** command shows a summarized list of the configured BGP neighbors as well as their status and statistics.

Router#show ip bgp summary

```
BGP router identifier 192.168.3.1, local AS number 304
8 network entries, 5 paths, and 23 BGP path attribute entries

   Neighbor      V       AS   MsgRcvd   MsgSent   InQ   OutQ   Up/Down     State/PfxRcd
   10.22.131.1   4       302  95        104       0     0      01:30:06        9
   10.22.131.9   4       302  97        105       0     0      01:30:07        21
   10.22.132.9   4       303  200       179       0     0      02:43:09        21
   10.22.134.1   4       304  166       178       0     0      02:43:15         3
   10.22.134.10  4       304  174       179       0     0      02:43:24         7
```

```
10.22.134.26   4         304       172         174         0       0       02:41:43          10
10.22.134.34   4         304       164         174         0       0       02:41:40           4
```

The following sample output of the **show ip bgp regexp _303_** command shows all of the entries in the BGP database that contain "303" in the AS path.

```
Router#show ip bgp regexp _303_
BGP local router ID is 192.168.3.1, local AS is 304.
Status codes: * valid, > best, i - internal, o - local
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            NextHop       Metric    LocPrf    Path
   10.22.130.8/29     10.22.132.9                       303 304 302 i
*  i10.22.130.240/28  0.22.132.1              100       303 300 i
*  10.22.130.240/28   10.22.132.9                       303 300 i
   10.22.131.0/29     10.22.132.9                       303 304 302 i
   10.22.131.8/29     10.22.132.9                       303 304 302 i
*  i10.22.131.16/29   10.22.132.1   0         100       303 i
*   10.22.131.16/29   10.22.132.9   0                   303 i
*  i10.22.131.240/28  10.22.132.1             100       303 300 i
*  10.22.131.240/28   10.22.132.9                       303 300 i
*  10.22.132.0/29     10.22.131.1   0                   302 303 i
*  10.22.132.0/29     10.22.131.9   0                   302 303 i
*  i10.22.132.0/29    10.22.132.1   0         100       303 i
*> 10.22.132.0/29     10.22.132.9   0                   303 i
*  10.22.132.8/29     10.22.131.1   0                   302 303 i
*  10.22.132.8/29     10.22.131.9   0                   302 303 i
*  10.22.132.8/29     10.22.132.9   0                   303 i
*  i10.22.132.240/28  10.22.132.1   0         100       303 i
*> 10.22.132.240/28   10.22.132.9   0                   303 i
   10.22.134.0/29     10.22.132.9                       303 304 i
   10.22.134.8/29     10.22.132.9                       303 304 i
   10.22.134.16/29    10.22.132.9                       303 304 i
   10.22.134.24/29    10.22.132.9                       303 304 i
   10.22.134.32/29    10.22.132.9                       303 304 i
   10.22.134.40/29    10.22.132.9                       303 304 i
   10.22.134.48/29    10.22.132.9                       303 304 i
   10.22.134.56/29    10.22.132.9                       303 304 i
   10.22.134.64/29    10.22.132.9                       303 304 i
   10.22.134.80/29    10.22.132.9                       303 304 i
   10.22.135.0/29     10.22.132.9                       303 304 305 i
   10.22.135.8/29     10.22.132.9                       303 304 305 i
Total RIB entries = 30
```

show ip bgp *<network ip>* [*</length>* | *<network-mask>*]

Use the **show ip bgp** *<network ip>* command to display details about the specified route, including the advertising router IP address, router ID, and the list of neighbors to which this route is being advertised.

Syntax Description

<network ip>	Shows only routes for the specified network.
</length>	Optional. Shows only routes for the specified network matching the prefix length (e.g., /24).
<network-mask>	Optional. Shows only routes for the specified network matching the network mask (e.g., 255.255.255.0).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example shows detailed output of this command:

```
>enable
#show ip bgp 10.15.240.0/28
BGP routing table entry for 10.15.240.0/28
Paths: (1 available, best #1)
 Advertised to peers:
 1.1.5.10
 100 1
  10.15.43.17 from 10.15.43.17 (8.1.1.1)
   Origin IGP, metric 2, valid, external, best
```

show ip bgp neighbors *<ip address>*

Use the **show ip bgp neighbors** command to display information for the specified Border Gateway Protocol (BGP) neighbor. Variations of this command include the following:

show ip bgp neighbors

show ip bgp neighbors *<ip address>*

show ip bgp neighbors *<ip address>* **[advertised-routes | received-routes | routes]**

Syntax Description

<ip address>	Displays information for the specified neighbor. If no IP address is entered, information for all neighbors is displayed.
advertised-routes	Displays all routes being advertised to the specified neighbor. Command output is the same as for **show ip bgp** except filtered to only the BGP routes being advertised to the specified neighbor.
received-routes	Displays all routes (accepted and rejected) advertised by the specified neighbor. Routes may be rejected by inbound filters such as prefix list filters.
routes	Displays all accepted received routes advertised by the specified neighbor. Routes displayed have passed inbound filtering. This command output is the same as **show ip bgp** except the output is filtered to those learned from the specified neighbor.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

Entries that are not filtered by prefix lists are marked with an asterisk (*) to show they are valid. Entries that are deemed the best path to advertised route are marked with a caret (>).

Usage Examples

The following are output variations of the **show ip bgp neighbors** command:

```
>enable
#show ip bgp neighbors
BGP neighbor is 10.15.43.17, remote AS 100, external link
Configured hold time is 180, keepalive interval is 60 seconds
Default minimum time between advertisement runs is 30 seconds
Connections established 6; dropped 5
Last reset: Interface went down
  Connection ID: 15
    BGP version 4, remote router ID 8.1.1.1
    BGP state is Established, for 01:55:05
    Negotiated hold time is 180, keepalive interval is 60 seconds
    Message statistics:
      InQ depth is 0, OutQ depth is 0
                    Local host: 10.15.43.18, Local port: 179
                                Sent            Rcvd
                    Opens:      1               1
                    Notifications: 0            0
                    Updates:    0               8
                    Keepalives: 116             116
                    Unknown:    0               0
                    Total:      117             125

Foreign host: 10.15.43.17, foreign port: 1048
    Flags: passive open

#show ip bgp neighbors 10.15.43.34 advertised-routes
BGP local router ID is 10.0.0.1, local AS is 101.
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          NextHop          Metric Path
*> 1.0.0.0/8        10.15.43.17         1 100 i
*> 2.0.0.0/9        10.15.43.17         1 100 i
```

```
#show ip bgp neighbors 10.15.43.17 received-routes
BGP local router ID is 10.0.0.1, local AS is 101.
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network           NextHop          Metric Path
*> 1.0.0.0/8         10.15.43.17           1 100 i
*> 2.0.0.0/9         10.15.43.17           1 100 i
```

```
#show ip bgp neighbors 10.15.43.17 routes
BGP local router ID is 10.0.0.1, local AS is 101.
Status codes: * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network           NextHop          Metric Path
*> 1.0.0.0/8         10.15.43.17           1 100 i
*> 2.0.0.0/9          10.15.43.17           1 100
```

show ip community-list [*<community-list-name>*]

Use the **show ip community-list** command to display any or all defined community lists in the router configuration.

Syntax Description

<community-list-name>	Optional. Specifies the name of the community list you wish to display. If this parameter is omitted, all defined community lists will be displayed.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example shows two community lists, one of which permits all routes containing community number 10:67, and another which permits routes containing community number 10:68 and the internet community number, but denies routes containing community number 10:45.

```
NetVanta4305#show ip community-list
ip community-list CommList1:
  permit 10:67
ip community-list CommList2:
  permit 10:68 internet
  deny 10:45
```

show ip dhcp-client lease *<interface>*

Use the **show ip dhcp-client lease** command to display all Dynamic Host Client Protocol (DHCP) lease information for interfaces that have dynamically assigned IP addresses.

Syntax Description

<interface>	Optional. Displays the information for the specified interface. Type **show ip dhcp-client lease ?** for a complete list of applicable interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following is a sample output from the **show dhcp-client lease** command:

```
>enable
#show dhcp-client lease

Interface: ethernet 0/1
  Temp IP address: 10.100.23.64 Mask: 0.0.0.0
  DHCP Lease server: 10.100.23.207 State: Bound (3)
  Lease: 120 seconds
 Temp default gateway address: 0.0.0.0
  Client-ID: N/A
```

show ip dhcp-server binding *<client ip address>*

Use the **show ip dhcp-server binding** command to display the Dynamic Host Client Protocol (DHCP) server client table with associated information.

Syntax Description

<client ip address>	Optional. Specifies a particular client IP address.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following is a sample output from the **show ip dhcp-server binding** command:

```
>enable
#show ip dhcp-server binding

IP Address      Client Id              Lease Expiration        Client Name
10.100.23.64    01:00:a0:c8:00:8f:b3   Aug 15 2002 11:02 AM    Router
```

show ip igmp groups *<group-address>*

Use the **show ip igmp groups** command to display the multicast groups that have been registered by directly connected receivers using Internet Group Management Protocol (IGMP). If no group address is specified, all groups are shown with this command.

Syntax Description

<group-address>	Optional. Displays the IP address of a multicast group.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following is sample output from this command:

```
>enable
#show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface       Uptime      Expires     Last Reporter
172.0.1.50       Loopback100     00:42:57    00:02:50    172.23.23.1
172.1.1.1        Ethernet0/1     00:05:26    00:02:51    1.1.1.2
172.1.1.1        Loopback100     00:42:57    00:02:51    172.23.23.1
```

show ip igmp interface *<interface>*

Use the **show ip igmp interface** command to display multicast-related information per-interface. If no interface is specified, this command shows information for all interfaces.

Syntax Description

<interface>	Displays information for a specific interface (in the format **type slot/port**). Enter the **show ip igmp interface ?** command for a complete list of interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.

Usage Examples

The following is sample output from this command:

```
>enable
#show ip igmp interface
eth 0/1 is UP
  Ip Address is 10.22.120.47, netmask is 255.255.255.0
  IGMP is enabled on interface
  Current IGMP version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  IGMP activity: 548 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP helper address is disabled
```

show ip interfaces [*<interface>* | brief]

Use the **show ip interfaces** command to display the status information for all IP interfaces (or a specific interface).

Syntax Description

<interface>	Optional. Displays status information for a specific interface. If no interface is entered, status information for all interfaces is displayed. Type **show ip interfaces ?** for a complete list of applicable interfaces.
brief	Displays an abbreviated version of interface statistics for all IP interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.
Release 11.1	Demand interface was added.

Usage Examples

The following is a sample output of the **show ip interfaces** command:

```
>enable
#show ip interfaces

eth 0/1 is UP, line protocol is UP
  Ip address is 10.10.10.1
  Netmask is 255.255.255.0
  MTU is 1500
  Fastcaching is Enabled
  RIP Authentication is Disabled
  RIP Tx uses global version value
  RIP Rx uses global version value
```

show ip local policy

Use the **show ip local policy** command to display information about the route-map used for local policy-based routing.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000, 5000, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Example

The following is sample output from this command:

```
>enable
#show ip local policy
Local policy routing is enabled, using route-map equal
route-map equal, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop 10.10.11.254
  Policy routing matches: 0 packets, 0 bytes
route-map equal, permit, sequence 20
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 10.10.11.14
  Policy routing matches: 2 packets, 172 bytes
```

show ip mroute [*<group-address>* | *<interface>*] [summary | all]

Use the **show ip mroute** command to display IP multicasting routing table information.

Syntax Description

<group-address>	Optional. Displays IP address of a multicast group.
<interface>	Optional. Displays the parameters for a specific interface (in the format **type slot/port**). For example: **eth 0/1**.
summary	Optional. Displays a single-line summary for each entry in the IP multicast routing table.
all	Optional: Displays all multicast routes, including those not used to forward multicast traffic.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.
Release 11.1	The All option was added.

Usage Examples

The following is sample output from the **show ip mroute** command:

```
>enable
#show ip mroute
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned, J - Join SPT, T - SPT-bit Set,
F - Register, R - RP-bit Set
Timers: Uptime/Expires

(*, 225.1.0.1), 01:16:21/00:02:45, RP 192.168.0.254, Flags: SC
  Incoming interface: tunnel 2, RPF nbr 172.16.2.10
  Outgoing interface list:
    eth 0/1, Forward, 01:16:21/00:02:45
```

The following is sample output from the **show ip mroute all** command:

```
>enable
#show ip mroute all
IP Multicast Routing Table
Flags: S - Sparse, C - Connected, P - Pruned, J - Join SPT, T - SPT-bit Set,
F - Register, R - RP-bit Set
Timers: Uptime/Expires

(*, 225.1.0.1), 01:17:34/00:03:25, RP 192.168.0.254, Flags: SC
  Forwarding Entry: Yes
  Incoming interface: tunnel 2, RPF nbr 172.16.2.10
  Outgoing interface list:
    eth 0/1, Forward, 01:17:34/00:03:25
```

show ip ospf

Use the **show ip ospf** command to display general information regarding open shortest path first (OSPF) processes.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is a sample output from the **show ip ospf** command:

```
>enable
#show ip ospf

Summary of OSPF Process with ID: 192.2.72.101
  Supports only single Type Of Service routes (TOS 0)
  SPF delay timer: 5 seconds, Hold time between SPFs: 10 seconds
  LSA interval: 240 seconds
  Number of external LSAs: 0, Checksum Sum: 0x0
  Number of areas: 0, normal: 0, stub: 0, NSSA: 0
```

show ip ospf database

Use the **show ip ospf database** command to display information from the open shortest path first (OSPF) database regarding a specific router. There are several variations of this command which you can use to obtain information about different OSPF link state advertisements. The variations are shown below:

show ip ospf *<area-id>* **database**
show ip ospf *<area-id>* **database adv-router** *<ip address>*
show ip ospf *<area-id>* **database database-summary**
show ip ospf *<area-id>* **database external** *<link-state-id>*
show ip ospf *<area-id>* **database external** *<link-state-id>* **adv-router** *<ip address>*
show ip ospf *<area-id>* **database network** *<link-state-id>*
show ip ospf *<area-id>* **database network** *<link-state-id>* **adv-router** *<ip address>*
show ip ospf *<area-id>* **database router** *<link-state-id>*
show ip ospf *<area-id>* **database router** *<link-state-id>* **adv-router** *<ip address>*
show ip ospf *<area-id>* **database summary** *<link-state-id>*
show ip ospf *<area-id>* **database summary** *<link-state-id>* **adv-router** *<ip address>*

Syntax Description

<area id>	Optional. Displays area ID number associated with the OSPF address range. This range is defined in the network router configuration command used to define the particular area. Refer to *network <ip address> <wildcard> area <area id>* on page 1122 for more information.
<link-state-id>	Optional. Identifies the portion of the Internet environment that is being described by the advertisement. The value needed in this field is tied to the advertisement's LS type.
<ip address>	Specifies the IP address in the form <A.B.C.D>.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The link state ID differs depending on whether the link state advertisement in question describes a network or a router.

If describing a network, this ID is one of the following:

- The network’s IP address. This is true for type 3 summary link advertisements and in autonomous system external link advertisements.
- An address obtained from the link state ID. If the network link advertisement’s link state ID is masked with the network’s subnet mask, this will yield the network’s IP address.

If describing a router, this ID is always the router’s OSPF router ID.

Usage Examples

```
>enable
#show ip ospf database
```

show ip ospf interface *<interface>*

Use the **show ip ospf interface** command to display open shortest path first (OSPF) information for a specific interface.

Syntax Description

<interface>	Optional. Displays the interface type. Type **show ip ospf interface ?** for a complete list of applicable interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.

Usage Examples

The following example shows OSPF information for the PPP 1 interface.

```
>enable
#show ip ospf interface ppp 1
```

show ip ospf neighbor *<interface> <neighbor id>* [detail]

Use the **show ip ospf neighbor** command to display open shortest path first (OSPF) neighbor information for a specific interface.

Syntax Description

<interface>	Optional. Displays the interface type. Type **show ip ospf neighbor ?** for a complete list of applicable interfaces.
<neighbor id>	Optional. Specifies a specific neighbor's router ID.
detail	Optional. Displays detailed information on all neighbors.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.

Usage Examples

The following example shows detailed information on the OSPF neighbors:

```
>enable
#show ip ospf neighbor
```

show ip ospf summary-address

Use the **show ip ospf summary-address** command to display a list of all summary address redistribution information for the system.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example displays all summary address redistribution information for the system:

```
>enable
#show ip ospf summary-address
```

show ip pim-sparse [interfaces *<interface>* | neighbor | rp-map | rp-set | state | traffic]

Use the **show ip pim-sparse** command to display Protocol Independent Multicast (PIM) configuration information. Sparse mode or PIM-SM is a routing protocol used to establish and maintain the multicast distribution tree. Routers can participate in the shared tree (RPT) rooted at the rendezvous point (RP) router or the shortest-path tree (SPT) rooted at a multicast source. PIM-SM also establishes both shared trees and shortest-path trees.

Syntax Description

interface *<interface>*	Displays PIM-SM configuration and status information for a specific interface. Type **show ip pim-sparse interface ?** to display a list of applicable interfaces.
neighbor	Displays neighbor adjacency information.
rp-map	Displays active group-to-RP mappings.
rp-set	Displays list of statically configured RP candidates. The group address is 224.0.0.0/4 when no access group was applied to the **rp-address** command (see *rp-address <ip address> access-group <access-list-name>* on page 1131). Otherwise it is the name of the access group.
state	Displays multicast route PIM state information.
traffic	Displays active PIM-SM control traffic statistics.

Default Values

No default necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and the Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example shows sample output from the **show ip pim-sparse** command:

```
>enable
#show ip pim-sparse
Global PIM Sparse Mode Settings
 Join/Prune interval: 60, SPT threshold: 1
```

The following example shows sample output from the **show ip pim-sparse interfaces** command:

```
>enable
#show ip pim-sparse interface

eth 0/1 is UP
  PIM Sparse
  DR: itself
  Local Address: 192.168.1.254
  Hello interval (sec): 30, Neighbor timeout (sec): 105
  Propagation delay (ms): 500, Override interval (ms): 2500

tunnel 1 is UP
  PIM Sparse
  DR: 172.16.1.10
  Local Address: 172.16.1.9
  Hello interval (sec): 30, Neighbor timeout (sec): 105
  Propagation delay (ms): 500, Override interval (ms): 2500

tunnel 2 is UP
  PIM Sparse
  DR: 172.16.2.10
  Local Address: 172.16.2.9
  Hello interval (sec): 30, Neighbor timeout (sec): 105
  Propagation delay (ms): 500, Override interval (ms): 2500
```

The following example shows sample output from the **show ip pim-sparse neighbor** command:

```
>enable
#show ip pim-sparse neighbor

Port           Neighbor        Holdtime(sec)  Age(sec)  Uptime(sec)
----------------------------------------------------------------------------------------------------
tunnel 1       172.16.1.10     105            19        241908
tunnel 2       172.16.2.10     105            23        241913
```

The following example shows sample output from the **show ip pim-sparse rp-map** command:

```
>enable
#show ip pim-sparse rp-map
Number of group-to-RP mappings: 5
Group address          RP address
---------------------------------------------------------
225.1.0.1              192.168.0.254
225.1.0.2              192.168.0.254
225.1.0.3              192.168.0.254
```

The following example shows sample output from the **show ip pim-sparse rp-map set** command:

```
>enable
#show ip pim rp-map set
Group address          Static-RP-address
--------------------------------------------------------------
224.0.0.0/4            192.168.0.254
MCAST_ACL_1            192.168.1.254
MCAST_ACL_2            192.168.2.254
MCAST_ACL_3            192.168.3.254
```

The following example shows sample output from the **show ip pim-sparse state** command:

```
>enable
#show ip pim-sparse state
PIM-SM State Table
Flags: S - Sparse, C - Connected, P - Pruned, J - Join SPT, T - SPT-bit Set,
F - Register, R - RP-bit Set
Timers: Uptime/Expires

(*, 225.1.0.1), 02:42:03/00:03:04, RP 192.168.0.254, Flags: SC
  Forwarding Entry: Yes
  Incoming interface: tunnel 2, RPF nbr 172.16.2.10
  Upstream Join/Prune State: Joined
  Register State: No Info
  RegStop Timer (sec): stopped
  Join/Prune Timer (sec): 57
  Override Timer (sec): stopped
  Multicast Border Router: 0.0.0.0
  Packets Forwarded: 2
  Outgoing interface list:
    eth 0/1, Forward, 02:42:03/00:03:03
      Downstream Join/Prune State: Join
      Assert Winner State: No Info
      Assert Timer (sec): stopped
      Assert Winner: 0.0.0.0
      Assert Winner Metric: infinity
      Local Membership: Yes
      Forwarding State: Forwarding
  Inherited output list:
    eth 0/1
```

The following example shows sample output from the **show ip pim-sparse traffic** command:

```
>enable
#show ip pim-sparse traffic
                      Rx             Tx                 Rx             Tx
Port: eth 0/1
  Hello:              7              8334      J/P:       0            0
  Register:           0              0         RegStop:   0            0
  Assert:             0              0
Port: tunnel 1
  Hello:              8327           8333      J/P:        0           57
  Register:           0              0         RegStop:    0           0
  Assert:             0              0
Port: tunnel 2
  Hello:              8323           8334      J/P:        0          11949
  Register:           0              0         RegStop:    0           0
  Assert:             0              0
Total
  Hello:              16657          25001     J/P:        0          12006
  Register:            0             0         RegStop:    0           0
  Assert:              0             0
```

show ip policy

Use the **show ip policy** command to display which route-map is associated with which interface for policy-based routing.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following is sample output from this command:

```
>enable
#show ip policy
Interface route-map
local       equal
Ethernet0/2   equal
Ethernet0/3   AAA-02/06/04-14:01:26.619-1-AppSpec (Dynamic)
```

show ip policy-class *<policyname>*

Use the **show ip policy-class** command to display a list of currently configured access policies. Refer to *ip policy-class <policyname> max-sessions <number>* on page 390 for information on configuring access policies.

Syntax Description

<policyname>	Optional. Displays policy class information for a specific policy class.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is a sample output from the **show ip policy-class** command:

```
>enable
#show ip policy-class

ip policy-class max-sessions 0

Policy-class "Trusted":
  0 current sessions (6000 max)
  Entry 1 - allow list MatchAll
```

show ip policy-sessions *<policyname>* [all]

Use the **show ip policy-sessions** command to display a list of current policy class associations. Refer to *ip policy-class <policyname> max-sessions <number>* on page 390 for information on configuring access policies.

Syntax Description

<policyname>	Optional. Displays policy class associations for a specific policy class.
all	Displays all policy-sessions, including active associations (through which the firewall is allowed to pass traffic) and associations flagged for deletion (through which the firewall is forbidden to pass traffic). Associations flagged for deletion will usually be freed within a few seconds of timeout or deletion, depending on packet congestion; servicing of packets is given priority. New traffic matching such an association will create a new active association, provided the traffic still matches a policy-class allow or NAT entry.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	The All option was added.

Usage Examples

The following is sample output from the **show ip policy-sessions** command:

```
>enable
#show ip policy-sessions

Protocol (TTL)
  Src IP Address      Src Port   Dest IP Address  Dst Port   NAT IP Address   NAT Port
  ------------------------------------------------------------------------------------------

Policy class "Public":
tcp (13)
  192.168.1.142       2621       192.168.19.2     1          10.10.10.1       3000
tcp (13)
  192.168.1.142       2622       192.168.19.2     2          10.10.10.1       3001
tcp (13)
  192.168.1.142       2623       192.168.19.2     3          10.10.10.1       3002
tcp (13)
  192.168.1.142       2624       192.168.19.2     4          10.10.10.1       3003
```

The following is sample output from the **show ip policy-sessions all** command:

```
>enable
#show ip policy-sessions all

Protocol (TTL)
  Src IP Address       Src Port  Dest IP Address  Dst Port   NAT IP Address   NAT Port
----------------------------------------------------------------------------------------------------

Policy class "Public":
tcp (0) - inactive
  192.168.1.142       1025       192.168.19.2     3135        10.10.10.1       3605
tcp (0) - inactive
  192.168.1.142       1028       192.168.19.2     3138        10.10.10.1       3606
tcp (0) - inactive
  192.168.1.142       1029       192.168.19.2     3139        10.10.10.1       3607
tcp (0) - inactive
  192.168.1.142       1036       192.168.19.2     3146        10.10.10.1       3608
```

show ip policy-stats *<policyname>*

Use the **show ip policy-stats** command to display a list of current policy class statistics. Refer to *ip policy-class <policyname> max-sessions <number>* on page 390 for information on configuring access policies.

Syntax Description

<policyname>	Optional. Displays policy class statistics for a specific policy class.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example displays a list of current policy class statistics:

```
>enable
#show ip policy-stats
```

show ip prefix-list [detail | summary] *<listname>*

Use the **show ip prefix-list** command to display BGP prefix list information.

Syntax Description

detail	Shows a listing of the prefix list rules and their hit counts.
summary	Shows information about the entire prefix list.
<listname>	Shows information for a specific prefix list.

Default Values

No default values are necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

If the **show ip prefix-list** command is issued with no arguments, a listing of the prefix-list rules but no hit count statistics is displayed.

Usage Examples

The following example displays information about the prefix list **test**.

```
>enable
#show ip prefix-list test

ip prefix-list test: 4 entries
  seq 5 permit 0.0.0.0/0 ge 8 le 8
  seq 10 deny 0.0.0.0/0 ge 9 le 9
  seq 15 permit 0.0.0.0/0 ge 10 le 10
  seq 20 deny 0.0.0.0/0 ge 11
```

show ip protocols

Use the **show ip protocols** command to display IP routing protocol parameters and statistics.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is a sample output from the **show ip protocols** command:

```
>enable
#show ip protocols

Sending updates every 30 seconds, next due in 8 seconds
  Invalid after 180 seconds, hold down time is 120 seconds
  Redistributing: rip
  Default version control: send version 2, receive version 2
  Interface     Send Ver.  Rec Ver.
    eth 0/1     2          2
    ppp 1       2          2
  Routing for networks:
    1.1.1.0/24
```

show ip route [connected | ospf | rip | static | table | bgp | summary | summary realtime | *<ip address> <subnet>*]

Use the **show ip route** command to display the contents of the IP route table.

Syntax Description

connected	Optional. Displays only the IP routes for directly connected networks.
ospf	Optional. Displays only the IP routes associated with OSPF.
rip	Optional. Displays only the IP routes that were dynamically learned through RIP.
static	Optional. Displays only the IP routes that were statically entered.
table	Optional. Displays a condensed version of the IP route table.
bgp	Displays only the IP routes associated with BGP.
summary	Optional. Displays a summary of all IP route information.
summary realtime	Optional. Displays full-screen output in realtime. See the **Functional Notes** below for more information.
<ip address><subnet>	Displays only the IP routes to destinations within the given address and subnet.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample output from the **show ip route** command:

```
>enable
#show ip route rip

Codes: C - connected S - static R - RIP O - OSPF IA - OSPF inter area
       N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1 E2 - OSPF external type 2

Gateway of last resort is 10.200.254.254 to network 0.0.0.0
```

The following example shows how to display IP routes learned via BGP. The values in brackets after a BGP route entry represent the entry's administrative distance and metric:

```
>enable
#show ip route bgp
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2

Gateway of last resort is 10.15.43.17 to network 0.0.0.0

B    1.0.0.0/8 [30/0] via 10.15.43.17, fr 1.17
B    2.0.0.0/9 [30/0] via 10.15.43.17, fr 1.17
B    2.128.0.0/10 [30/0] via 10.15.43.17, fr 1.17
B    2.192.0.0/11 [30/0] via 10.15.43.17, fr 1.17
B    2.224.0.0/12 [30/0] via 10.15.43.17, fr 1.17
B    2.240.0.0/13 [30/0] via 10.15.43.17, fr 1.17
B    2.248.0.0/14 [30/0] via 10.15.43.17, fr 1.17
```

show ip traffic [realtime]

Use the **show ip traffic** command to display all IP traffic statistics.

Syntax Description

realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

```
>enable
#show ip traffic
```

show lldp

Use the **show lldp** command to display local loop demarkation point (LLDP) timer configuration.

Syntax Description

No subcommands.

Default Values

No default values are necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example shows a sample LLDP timer configuration:

```
>enable
#show lldp
Global LLDP information:
Sending LLDP packets every 30 seconds
Sending TTL of 120 seconds
```

show lldp device *<system name>*

Use the **show lldp device** command to display specific neighbor information about a given neighbor.

Syntax Description

<system name>	Specifies the system name of the neighbor to display.

Default Values

No default values are necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

If there is more than one neighbor with the same system name, all neighbors with that system name will be displayed.

Usage Examples

The following example shows specific information about a neighbor for the system name **Router**:

```
>enable
#show lldp device Router

Chassis ID: 00:A0:C8:02:DD:2A (MAC Address)
                    System Name: Router
                    Device Port: eth 0/1 (Locally Assigned)
                    Holdtime: 30
                    Platform: NetVanta 3305
                    Software: Version: 08.00.22.sw1.D, Date: Mon Nov 01 10:28:55 2004
                    Capabilities: Bridge, Router
                    Enabled Capabilities: Router
                    Local Port: eth 0/3
                    Management Addresses:
                    Address Type: IP version 4, Address: 10.23.10.10
                    Interface Type: Interface Index, Interface Id: 2
```

show lldp interface *<interface>*

Use the **show lldp interface** command to display local loop demarkation point (LLDP) configuration and statistics for interfaces on this device.

Syntax Description

<interface>	Displays the information for the specified interface. Type **show lldp interface ?** for a complete list of applicable interfaces.

Default Values

No default values are necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example shows LLDP configuration and statistics for the Ethernet 0/1 interface:

```
>enable
#show lldp interface ethernet 0/1
eth 0/1 (TX/RX)
  0 packets input
    0 input errors
    0 TLV errors, 0 TLVs Discarded
    0 packets discarded
  8799 packets output
  0 neighbor ageouts
#
```

show lldp neighbors [interface *<interface>* | *<interface type>* | detail | realtime]

Use the **show lldp neighbors interface** command to display information about neighbors of this device learned about via local loop demarkation point (LLDP).

Syntax Description

<interface>	Displays a summary of all neighbors learned about through the specified interface (e.g., **eth 0/1**). Type **show lldp neighbors interface ?** for a complete list of applicable interfaces.
<interface type>	Displays a summary of all neighbors learned about through interfaces of the specified type (e.g., **eth**).
detail	Optional. Shows detailed neighbor information for the specified interface or interface type.
realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following example shows detailed information about a device’s neighbors:

```
>enable
#show lldp neighbors interface eth 0/3 detail
Chassis ID: 00:A0:C8:02:DD:2A (MAC Address)
 System Name: Router
 Device Port: eth 0/1 (Locally Assigned)
 Holdtime: 38
 Platform: NetVanta 3305
  Software: Version: 08.00.22.sw1.D, Date: Mon Nov 01 10:28:55 2004
  Capabilities: Bridge, Router
  Enabled Capabilities: Router
 Local Port: eth 0/3
 Management Addresses:
   Address Type: IP version 4, Address: 10.23.10.10
   Interface Type: Interface Index, Interface Id: 2
```

show lldp neighbors statistics

Use the **show lldp neighbors statistics** command to display statistics about local loop demarkation point (LLDP) neighbor table actions.

Syntax Description

No subcommands.

Default Values

There are no default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command shows information about the changes in this device’s neighbor table. The information displayed indicates the last time a neighbor was added to or removed from the table as well as the number of times neighbors were inserted into or deleted from the table.

Usage Examples

The following example shows sample output for this command:

```
>enable
#show lldp neighbors statistics
System Last Change Time    Inserts     Deletes     Drops       Age outs
10-15-2004 14:24:56        55          3           1           1
```

System Last Change Time - Shows the time at which the most recent change occurred in the neighbor table.

Inserts - Shows the number of times neighbors have been added to the table.

Deletes - Shows how many times neighbors have been deleted from the table because an interface was shut down.

Drops - Shows how many times the insertion of a new neighbor into the table failed because the table was full.

Age outs - Shows how many times neighbors have been removed from the table because no new updates were received from that neighbor before its time-to-live timer expired.

show memory [heap | realtime | uncached-heap]

Use the **show memory** command to display statistics regarding memory including memory allocation and buffer use statistics. Shows how memory is in use (broken down by memory size) and how much memory is free.

Syntax Description

heap	Shows how much memory is in use (broken down by memory block size) and how much memory is free.
uncached-heap	Shows how much memory has been set aside to be used without memory caching, how much memory is being used and how much memory is free. (Valid only on NetVanta 300, 1000, and 1000R Series Units.)
realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 10.1	Realtime option was introduced.
Release 11.1	Uncached heap option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample output from the **show memory heap** command:

```
>enable
#show memory heap

Memory Heap:
  HeapFree: 2935792
  HeapSize: 8522736

Block Managers:
Mgr          Size    Used  Free          Max-Used
0            0       58    0             58
1            16      1263  10            1273
2            48      1225  2             1227
3            112     432   2             434
4            240     140   3             143
5            496     72    2             74
6            1008    76    1             26
7            2032    25    1             26
8            4080    2     1             3
9            8176    31    1             32
10           16368   8     0             8
11           32752   5     1             6
12           65520   3     0             30
13           131056  0     0             0
```

show modules [verbose]

The **show modules** command displays information on the current system setup.

Syntax Description

verbose	Enables detailed messaging.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, and 5000 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example displays the modules installed in the unit.

```
>enable
#show modules

   Slot        Ports        Type            Serial #       Part #        H/W Rev
 --------------------------------------------------------------------------------
    0            3      Netvanta 5305     ***********    1200990L1          A
    1            1       T3 Module        ***********    1200832L1          A
    2            -         Empty          -----------    -----------    ----------
    3            -         Empty          -----------    -----------    ----------
    4            -         Empty          -----------    -----------    ----------
    5            -         Empty          -----------    -----------    ----------
    6            -         Empty          -----------    -----------    ----------
    7            -         Empty          -----------    -----------    ----------
```

show output-startup

Use the **show output-startup** command to display startup configuration output line-by-line. This output can be copied into a text file and then used as a configuration editing tool.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following is a sample output from the **show output-startup** command:

```
>enable
#show output-startup

!
#!
#hostname "UNIT_2"
UNIT_2#no enable password
UNIT_2#!
UNIT_2#ip subnet-zero
UNIT_2#ip classless
UNIT_2#ip routing
UNIT_2#!
UNIT_2#event-history on
UNIT_2#no logging forwarding
UNIT_2#logging forwarding priority-level info
UNIT_2#no logging email
etc....
```

show power supply

The **show power supply** command displays the power supply status.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example displays the power supply status:

```
>enable
#show power supply

Power supply 1 is OK.

Power supply 2 is not present.
```

show pppoe

Use the **show pppoe** command to display all point-to-point over Ethernet (PPPoE) settings and associated parameters.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example enters the Enable mode and uses the **show** command to display PPPoE information:

```
>enable
#show pppoe
ppp 1
  Outgoing Interface: eth 0/1
  Outgoing Interface MAC Address: 00:A0:C8:00:85:20
  Access-Concentrator Name Requested: FIRST VALID
  Access-Concentrator Name Received: 13021109813703-LRVLGAOS90W_IFITL
  Access-Concentrator MAC Address: 00:10:67:00:1D:B8
  Session Id: 64508
  Service Name Requested: ANY
  Service Name Available:
  PPPoE Client State: Bound (3)
 Redial retries:   unlimited
  Redial delay:     10 seconds
Backup enabled all day on the following days:
     Sunday Monday Tuesday Wednesday Thursday Friday Saturday
  Backup phone number list:
    Number              Call Type   min/max DS0s   Backup I/F
    5551212               analog       1/1           ppp 2
```

show processes [cpu | cpu realtime | history | queue | stack]

Use the **show processes** command to display process statistic information.

Syntax Description

cpu	Displays informations about processes that are currently active.
cpu realtime	Displays full-screen CPU output in real time. See the *Functional Notes* below for more information.
history	Displays the process switch history.
queue	Displays process queue utilization.
stack	Displays process stack usage.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 10.1	New option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample output from the **show processes cpu** command:

```
>enable
#show processes cpu
```

```
processes cpu
System load: 7.07%     Min: 0.00%     Max 85.89%
Context switch load: 0.21%
```

```
Task    Task            Invoked     Exec      Time     Runtime   Load %
D       Name            PRI STAT    (count)   (usec)   (usec)    (1sec)
0       Idle            0 W         129689    1971     927923    92.79
1       FrontPanel      249 W       9658      165      3202      0.32
3       Stack Usage     11 W        485       305      325       0.03
4       Q Test 1        10 W        50        4        0         0.00
5       Q Test 2        11 W        50        6        0         0.00
10      Clock           20 W        1443      24       55        0.01
11      PacketRouting   250 W       31656     10       3871      0.39
12      Thread Pool     50 W        161       159      0         0.00
13      IKE             10 W        2         341      0         0.00
14      RouteTableTick  50 W        49        874      874       0.09
....etc.
```

show qos map

The **show qos map** command outputs information about the quality of service (QoS) map. This information differs based on how a particular map entry is defined.

Variations of this command include the following:

show qos map
show qos map *<map name>*
show qos map *<map name> <sequence number>*
show qos map interface *<interface id>*

Syntax Description

<map name>	Specifies the name of a defined QoS map.
<sequence number>	Specifies one of the map's defined sequence numbers.
<interface id>	Displays the QoS map information for a specific interface (e.g., Frame Relay, PPP, or ATM). Enter the **show qos map interface ?** command for a complete list of interfaces.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC interface.
Release 11.1	Demand interface was added.

Usage Example

```
>enable
#show qos map
qos map priority
map entry 10
   match IP packets with a precedence value of 6
   priority bandwidth: 400 (kilobits/sec) burst: default
   packets matched by map: 125520

  map entry 20
   match ACL icmp
   packets matched by map: 99

  map entry 30
   match RTP packets on even destination ports between 16000 and 17000
   packets matched by map: 0

  map entry 50
   match ACL tcp
   packets matched by map: 4326

  map entry 60
  match IP packets with a dscp value of 2
  set dscp value to 6
  packets matched by map: 0

  map entry 70
  match NetBEUI frames being bridged by the router
  priority bandwidth: 150 (kilobits/sec) burst: default
  packets matched by map: 0



  qos map tcp_map
  map entry 10
   match ACL tcp
   priority bandwidth: 10 (kilobits/sec) burst: default
   set precedence value to 5
   packets matched by map: 0

  map entry 20
   match IP packets with a precedence value of 3
   priority bandwidth: 50 (kilobits/sec) burst: default
   packets matched by map: 0
```

The following example shows the “priority” Qos Map and all entries in that map:

```
>enable
#show qos map priority

  qos map priority
  map entry 10
   match IP packets with a precedence value of 6
   priority bandwidth: 400 (kilobits/sec) burst: default
   packets matched by map: 125520

  map entry 20
   match ACL icmp
   packets matched by map: 99

  map entry 30
   match RTP packets on even destination ports between 16000 and 17000
   packets matched by map: 0

  map entry 50
   match ACL tcp
   packets matched by map: 4326

  map entry 60
   match IP packets with a dscp value of 2
   set dscp value to 6
   packets matched by map: 0

  map entry 70
   match NetBEUI frames being bridged by the router
   priority bandwidth: 150 (kilobits/sec) burst: default
   packets matched by map: 0
```

The following example shows a particular qos map entry (in this case map entry 10):

```
>enable
#show qos map priority 10

  qos map priority
  map entry 10
   match IP packets with a precedence value of 6
   priority bandwidth: 400 (kilobits/sec) burst: default
   packets matched by map: 125520
```

The following examples show Qos Map interface stats associated with the map defined for an interface:

```
>enable
#show qos map interface frame-relay 1
fr 1
qos-policy out: priority



    map entry 10
     match IP packets with a precedence value of 6
     budget 145/10000 bytes (current/max)
     priority bandwidth: 400 (kilobits/sec)
     packets matched on interface: 27289
     packets dropped: 98231

    map entry 20
    not configured for rate limiting

    map entry 30
    not configured for rate limiting

    map entry 50
    not configured for rate limiting

    map entry 60
    not configured for rate limiting

    map entry 70
     match NetBEUI frames being bridged by the router
     budget 3750/3750 bytes (current/max)
     priority bandwidth: 150 (kilobits/sec)
     packets matched on interface: 0
     packets dropped: 0
```

show queue *<interface>*

Use the **show queue** command to display conversation information associated with an interface queue. This command shows summary and per-conversation information.

Syntax Description

<interface>	Displays the queueing information for the specified interface. Type the **show queue ?** command to display a list of valid interfaces.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC interface.
Release 11.1	Demand interface was added.

Usage Examples

The following is a sample output from the **show queue** command:

```
>enable
#show queue fr 1

Queueing method: weighted fair
  Output queue: 18/25/200/64/1027 (size/highest/max total/threshold/drops)
    Conversations 2/4/256 (active/max active/max total)

  (depth/weight/highest/discards) 12/256/33/0
  Conversation 10, linktype: ip, length: 67
  source: 10.100.23.11, destination: 10.200.2.125, id: 0x0000, ttl: 47,
  TOS: 0 prot: 17 (udp), source port 99, destination port 99

  (depth/weight/highest/discards) 6/256/25/0
  Conversation 23, linktype: ip, length: 258
  source: 10.100.23.11, destination: 10.200.2.125, id: 0x0000, ttl: 47,
  TOS: 0 prot: 6 (tcp), source port 16, destination port 16
```

show queuing [fair]

Use the **show queuing** command to display information associated with configured queuing methods.

Syntax Description

fair	Optional. Displays only information on the weighted fair queuing configuration.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following is a sample output from the **show queuing** command:

```
>enable
#show queuing

 Interface    Discard threshold    Conversation subqueues
   fr 1              64                       256
   fr 2              64                       256
  ppp 1              64                       256
```

show radius statistics

Use the **show radius statistics** command to display various statistics from the RADIUS subsystem. These statistics include number of packets sent, number of invalid responses, number of timeouts, average packet delay, and maximum packet delay. Statistics are shown for both authentication and accounting packets.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following is an example output using the **show radius statistics** command:

```
>enable
#show radius statistics

                                  Auth.           Acct.
Number of packets sent:           3               0
Number of invalid responses:      0               0
Number of timeouts:               0               0
Average delay:                    2 ms            0 ms
Maximum delay:                    3 ms            0 ms
```

show route-map [<*name*>]

Use the **show route-map** command to display any route-maps that have been configured in the router. It displays any match and set clauses associated with the route-map, as well as the number of incoming routes that have matched each route-map. Route-maps can be used for BGP and PBR.

Syntax Description

<*name*>	Optional. Displays only the route-map matching the specified name.

Default Values

By default, this command displays all defined route-maps.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

In the example below, all route-maps in the router are displayed.

```
>enable
#show route-map
route-map RouteMap1, permit, sequence 10
  Match clauses:
    community (community-list filter): CommList1
  Set clauses:
    local-preference 250
  BGP Filtering matches: 75 routes
  Policy routing matches: 0 packets 0 bytes
route-map RouteMap1, permit, sequence 20
  Match clauses:
    community (community-list filter): CommList2
  Set clauses:
    local-preference 350
  BGP Filtering matches: 87 routes
  Policy routing matches: 0 packets 0 bytes
route-map RouteMap2, permit, sequence 10
```

```
  Match clauses:
    ip address (access-lists): Acl1
  Set clauses:
    metric 100
  BGP Filtering matches: 10 routes
  Policy routing matches: 0 packets 0 bytes
route-map RouteMap2, permit, sequence 20
  Match clauses:
    ip address (access-lists): Acl2
  Set clauses:
    metric 200
  BGP Filtering matches: 12 routes
  Policy routing matches: 0 packets 0 bytes
route-map RouteMap3, permit, sequence 10
  Match clauses:
    length 150 200
  Set clauses:
    ip next-hop: 10.10.11.254
  BGP Filtering matches: 0 routes
  Policy routing matches: 0 packets 0 bytes
route-map RouteMap3, permit, sequence 20
  Match clauses:
    ip address (access-lists): Acl3
  Set clauses:
    ip next-hop: 10.10.11.14
  BGP Filtering matches: 0 routes
  Policy routing matches: 144 packets 15190 bytes
```

In the example below, only RouteMap2 is displayed.

```
#show route-map RouteMap2
route-map RouteMap2, permit, sequence 10
  Match clauses:
    ip address (access-lists): Acl1
  Set clauses:
    metric 100
  BGP Filtering matches: 10 routes
  Policy routing matches: 0 packets 0 bytes
route-map RouteMap2, permit, sequence 20
  Match clauses:
    ip address (access-lists): Acl2
```

```
 Set clauses:
   metric 200
 BGP Filtering matches: 12 routes
 Policy routing matches: 0 packets 0 bytes
```

In the example below, only RouteMap3 is displayed.

```
#show route-map RouteMap3
route-map RouteMap3, permit, sequence 10
 Match clauses:
   length 150 200
 Set clauses:
   ip next-hop: 10.10.11.254
 BGP Filtering matches: 0 routes
 Policy routing matches: 0 packets 0 bytes
route-map RouteMap3, permit, sequence 20
 Match clauses:
   ip address (access-lists): Acl3
 Set clauses:
   ip next-hop: 10.10.11.14
 BGP Filtering matches: 0 routes
 Policy routing matches: 144 packets 15190 bytes
```

show running-config

Use the **show running-config** command to display a text print of all the non-default parameters contained in the current running configuration file. Specific portions of the running-config may be displayed, based on the command entered.

Variations of this command include the following:

show running-config
show running-config access-lists
show running-config access-lists verbose
show running-config checksum
show running-config interface *<interface type> <interface id>*
show running-config interface *<interface type> <interface id>* **verbose**
show running-config ip-crypto
show running-config ip-crypto verbose
show running-config policy-class
show running-config policy-class verbose
show running-config qos-map
show running-config qos-map verbose
show running-config router pim-sparse
show running-config router pim-sparse verbose
show running-config verbose

Syntax Description

access-lists	Displays the current running configuration for all configured IP access lists.
checksum	Optional. Displays the encrypted Message Digest 5 (MD5) version of the running configuration.
interface *<interface type>*	Displays the current running configuration for a particular interface. Type **show running-config interface ?** for a list of valid interfaces.
<interface id>	Specifies any valid slot/port interface (e.g., 0/1).
ip crypto	Displays the current running configuration for all IPSec VPN settings.
policy-class	Displays the current running configuration for all configured policy classes.
qos-map	Displays the current running configuration for all configured QoS maps.
router pim-sparse	Optional: Displays the current global PIM-SM configuration.
verbose	Optional. Displays the entire running configuration to the terminal screen (versus only the non-default values).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include HDLC and tunnel interfaces.
Release 11.1	Demand, FXO, and serial interfaces were added. IP crypto and router pim-sparse key words were added.

Usage Examples

The following is a sample output from the **show running-config** command:

```
>enable
#show running-config
Building configuration...
!
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
logging forwarding priority-level info
no logging email
!
ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
!
interface eth 0/1........
```

show sip [resources | statistics | trunk-registration | user-registration]

Use the **show sip** command to display Session Initiation Protocol (SIP) statistical and registration information.

Syntax Description

resources	Displays SIP server statistic information.
statistics	Displays SIP server statistic information.
trunk-registration	Displays local SIP client registration information.
user-registration	Displays local SIP server registration information.

Default Values

No default necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.
Release 11.1	Resources, statistics, and user-registration options were added.

Usage Examples

The following example shows sample output from the **show sip trunk-registration** command:

```
>enable
#show sip trunk-registration

Ext     Register  Expire  Grant  Success  Redirect  Challenge  Failed  Timeout
------------------------------------------------------------------------------------------------------------------
4433     NO         0       0       0        0          0        0       #
```

show sip location [dynamic | static]

Use the **show sip location** command to display Session Initiation Protocol (SIP) statistical and registration information.

Syntax Description

dynamic	Displays SIP location database dynamic entries.
static	Displays SIP location database static entries.

Default Values

No default necessary for this command.

Applicable Platforms

This command applies to the Total Access 2000 and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example shows sample output from the **show sip location static** command:

```
>enable
#show sip location static
User            IP Address      Port    Expires    Source
------------------------------------------------------------------------------------------------
Test            10.1.1.1        5060          0    User Config
```

show snmp

Use the **show snmp** command to display the system Simple Network Management Protocol (SNMP) parameters and current status of SNMP communications.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is an example output using the **show snmp** command for a system with SNMP disabled and the default Chassis and Contact parameters:

```
>enable
#show snmp

Chassis: Chassis ID
Contact: Customer Service
0 Rx SNMP packets
   0 Bad community names
   0 Bad community uses
   0 Bad versions
   0 Silent drops
   0 Proxy drops
   0 ASN parse errors
```

show sntp

Use the **show sntp** command to display the system Simple Network Time Protocol (SNTP) parameters and current status of SNTP communications.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

```
>enable
#show sntp
```

show spanning-tree *<bridgegroup#>*

Use the **show spanning-tree** command to display the status of the spanning-tree protocol.

Syntax Description

<bridgegroup#>	Optional. Displays spanning-tree for a specific bridge group.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following is an example output using the **show spanning-tree** command:

```
>enable
#show spanning-tree

Spanning Tree enabled protocol ieee
  Root ID    Priority     32768
             Address      00:a0:c8:00:88:41
             We are the root of the spanning tree
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority     32768
             Address      00:a0:c8:00:88:41
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   300
Interface           Role                Sts                 Cost        Prio.Nbr      Type
-------------------  -------------------  -------------------  -----------  -------------  ---------------
eth 0/2             Desg                FWD                 19          128.2         P2p
eth 0/3             Desg                FWD                 19          128.3         P2p
eth 0/4             Desg                FWD                 19          128.4         P2p
giga-eth 0/1        Desg                FWD                 4           128.25        P2p
giga-eth 0/2        Desg                FWD                 4           128.26        P2p
```

show startup-config

Use the **show startup-config** command to display a text printout of the startup configuration file stored in NVRAM.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample output of the **show startup-config** command:

```
>enable
#show startup-config
!
!
no enable password
!
ip subnet-zero
ip classless
ip routing
!
event-history on
no logging forwarding
logging forwarding priority-level info
no logging email
!
ip policy-timeout tcp all-ports 600
ip policy-timeout udp all-ports 60
ip policy-timeout icmp 60
!
```

```
!
!
interface eth 0/1
speed auto
  no ip address
  shutdown
!
interface dds 1/1
  shutdown
!
interface bri 1/2
  shutdown
!
!
ip access-list standard MatchAll
  permit host 10.3.50.6
  permit 10.200.5.0 0.0.0.255
!
!
ip access-list extended UnTrusted
  deny   icmp 10.5.60.0 0.0.0.255 any source-quench
  deny   tcp any any
!
no ip snmp agent
!
!
!
```

show startup-config checksum

Use the **show startup-config checksum** command to display the Message Digest 5 (MD5) checksum of the unit’s startup configuration.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command is used in conjunction with the **show running-config checksum** command to determine whether the configuration has changed since the last time it was saved.

Usage Examples

The following example displays the MD5 checksum of the unit’s startup configuration:

```
>enable
#show startup-config checksum
10404D5DAB3FE35E307B6A79AC6AC8C0
#

#show running-config checksum
10404D5DAB3FE35E307B6A79AC6AC8C0
#
```

show system

The **show system** command shows the system version, timing source, power source, and alarm relay status.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following is sample output for this command:

```
>enable
#show system
ADTRAN, Inc. OS version 07.00.20
  Checksum: 3B2FCC0F, built on Tue Jun 01 13:36:36 2004
Boot ROM version 07.00.20
  Checksum: 604D, built on: Tue Jun 01 13:59:11 2004
Copyright (c) 1999-2004, ADTRAN, Inc.
Platform: Total Access 900
Serial number TechPub
Flash: 8388608 bytes  DRAM: 33554431 bytes
ICP uptime is 0 days, 0 hours, 53 minutes, 50 seconds
System returned to ROM by External Hard Reset
Current system image file is "070020.biz"
Boot system image file is "070020.biz"
Power Source:  AC
Primary System clock source config:  t1 0/1
Secondary System clock source config:  t1 0/1
Active System clock source:  t1 0/1
Alarm Relay:  OPEN
```

show tacacs+ statistics

Use the **show tacacs+ statistics** command to display terminal access controller access control system (TACACS+) client statistics.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

```
>enable
#show tacacs+ statistics

                        Authentication   Authorization   Accounting
Packets sent:           0                0               0
Invalid responses:      0                0               0
Timeouts:               0                0               0
Average delay:          0ms              0ms             0ms
Maximum delay:          0ms              0ms             0ms

Socket Opens:                 0
Socket Closes:                0
Socket Aborts:                0
Socket Errors:                0
Socket Timeouts:              0
Socket Failed Connections:    0
Socket Packets Sent:          0
Socket Packets Received:      0
```

show tcp info [realtime] *<control block>*

Use the **show tcp info** command to display Transmission Control Protocol (TCP) control block information in the AOS. This information is for troubleshooting and debug purposes only. For more detailed information, you can optionally specify a particular TCP control block. When a particular TCP control block is specified, the system provides additional information regarding crypto map settings that the **show tcp info** command does not display.

Syntax Description

realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.
<control block>	Optional. Specifies a particular TCP control block for more detailed information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Function Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample from the **show tcp info** command:

```
>enable
#show tcp info

TCP TCB Entries
```

Usage Examples

```
ID   STATE   LSTATE  OSTATE  TYPE   FLAGS  RPORT  LPORT  SWIN  SRT  INTERFACE
 0   FREE    FREE    FREE    SRVR     0      0      0      0    0     NONE
 1   LISTEN  FREE    FREE    CONN     0      0     21      0    0     NONE
 2   LISTEN  FREE    FREE    CONN     0      0     80      0    0     NONE
 3   LISTEN  FREE    FREE    CONN     0      0     23      0    0     NONE
 4   LISTEN  FREE    FREE    CONN     0      0   5761      0    0     NONE
 5   FREE    FREE    FREE    SRVR     0      0      0      0    0     NONE
 .
 .
31   FREE    FREE    FREE    SRVR     0      0      0      0    0     NONE
```

show temperature

Use the **show temperature** command to display the unit temperature.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following is sample output from the **show temperature** command:

```
>enable
#show temperature

Temperature: 33 degrees C
```

show thresholds

Use the **show thresholds** command to display thresholds currently crossed for all DS1 interfaces.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

```
>enable
#show thresholds

t1 1/1:
    SEFS 15 min threshold exceeded
    UAS 15 min threshold exceeded
    SEFS 24 hr threshold exceeded
    UAS 24 hr threshold exceeded
t1 1/2:
    No thresholds exceeded
```

show users [realtime]

Use the **show users** command to display the name (if any) and state of users authenticated by the system. Displayed information includes:

- Connection location (for remote connections this includes Transmission Control Protocol (TCP) information)
- Username of authenticated user
- Current state of the login (in process or logged in)
- Current enabled state
- Time the user has been idle on the connection

Syntax Description

realtime	Displays full-screen output in real time. See the *Functional Notes* below for more information.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 10.1	The real time display option was introduced.

Functional Notes

Use the **realtime** argument for this command to display full-screen output in real time. Information is continuously updated on the console until you either freeze the data (by pressing the **F** key) or exit **realtime** mode (by pressing **Ctrl-C**). If there is not enough room on the screen for all available data, the information will truncate at the bottom of the screen. In order to maximize the amount of data displayed, increase the terminal length (using the **terminal length** command; refer to *terminal length <text>* on page 276).

Usage Examples

The following is a sample of **show users** output:

```
>enable
#show users

- CONSOLE 0 'adtran' logged in and enabled
  Idle for 00:00:00
- TELNET 0 (172.22.12.60:3998) 'password-only' logged in (not enabled)
  Idle for 00:00:14
- FTP (172.22.12.60:3999) 'adtran' logged in (not enabled)
  Idle for 00:00:03
```

show version

Use the **show version** command to display the current ADTRAN operating system (AOS) version information.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample **show version** output:

```
>enable
#show version

AOS version: 02.01.00
Checksum: 1505165C Built on: Fri Aug 23 10:23:13 2002
 Upgrade key: 420987gacs9097gbdsado
BootROM version: 02.01.00
 Checksum: DB85 Built on: Mon Aug 19 10:33:03 2002
Copyright 1999-2002 ADTRAN Inc.
Serial number b104

Router uptime is 0 days 3 hours 9 minutes 54 seconds
System returned to ROM by External Hard Reset
System image file is "020100.biz"
```

sip check-sync

Use the **sip check-sync** command to send a check-sync notification to all IP phones registered to the unit. When an IP phone receives this check-sync notification, the phone will check for possible configuration changes stored on the server.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example notifies all IP phones to check for a change in configuration:

```
>enable
#sip check-sync
```

telnet *<address>*

Use the **telnet** command to open a Telnet session (through the AOS) to another system on the network.

Syntax Description

<address>	Specifies the IP address of the remote system.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example opens a Telnet session with a remote system (**10.200.4.15**):

```
>enable
#telnet 10.200.4.15

User Access Login:

Password:
```

terminal length *<text>*

The **terminal length** command sets the number of rows (lines) for a terminal session. Use the **no** form of this command to return to the default value. This command is only valid for the current session and returns to the default (24 rows) when the session closes.

Syntax Description

No subcommands.

Default Values

The default setting for this command is 24 rows.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sets the number of rows to 30.

```
>enable
#terminal length 30
```

traceroute *<address>* source *<address>*

Use the **traceroute** command to display the IP routes a packet takes to reach the specified destination.

Syntax Description

<address>	Optional. Specifies the IP address of the remote system to trace the routes to.
source *<address>*	Optional. Specifies the IP address of the interface to use as the source of the trace.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following is a sample **traceroute** output:

```
>enable
#traceroute 192.168.0.1

Type CTRL+C to abort.
Tracing route to 192.168.0.1 over a maximum of 30 hops

  1   22ms   20ms   20ms    192.168.0.65
  2   23ms   20ms   20ms    192.168.0.1
#
```

The following example specifies the source of the trace. The ip address **10.10.10.10** is the destination address:

```
>enable
#traceroute 10.10.10.10 source 192.168.0.3
```

undebug all

Use the **undebug all** command to disable all activated debug messages.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example disabled all activated debug messages:

```
>enable
#undebug all
```

wall *<message>*

Use the **wall** command to send messages to all users currently logged in to the AOS unit.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sends the message “Reboot in 5 minutes if no objections” to the CLI screen of everyone currently connected:

```
>enable
#wall Reboot in 5 minutes if no objections
```

write [dynvoice-config | erase | memory | network | terminal]

Use the **write** command to save the running configuration to the unit's nonvolatile random access memory (NVRAM) or a Trivial File Transfer Protocol (TFTP) server. Also use the **write** command to clear NVRAM or to display the running configuration on the terminal screen. Entering the **write** command with no other arguments copies your configuration changes to the unit's NVRAM. Once the save is complete, the changes are retained even if the unit is shut down or suffers a power outage.

Syntax Description

dynvoice-config	Optional. Writes dynvoice configuration information to the unit's NVRAM.
erase	Optional. Erases the configuration files saved to the unit's NVRAM.
memory	Optional. Saves the current configuration to NVRAM. Refer to *copy <source> <destination>* on page 83 for more information.
network	Optional. Saves the current configuration to the network TFTP server. Refer to *copy tftp <destination>* on page 87 for more information.
terminal	Optional. Displays the current configuration on the terminal screen.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example saves the current configuration to the unit's NVRAM:

```
>enable
#write memory
```

GLOBAL CONFIGURATION MODE COMMAND SET

To activate the Global Configuration mode, enter the **configuration** command at the Enable Security mode prompt. For example:

```
>enable
#configure terminal
(config)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

aaa accounting commands begin on page 284
aaa authentication commands begin on page 287
aaa authorization commands begin on page 292
aaa group server [radius | tacacs+] <listname> on page 294
aaa on on page 296
aaa processes <threads> on page 298
arp <ip address> <mac address> arpa on page 299
auto-config [filename <name> | restart | retry-count <number>| server <name or address>] on page 300
banner [exec | login | motd] <character> <message> <character> on page 302
boot system flash <filename> [no-backup | <backup filename>] on page 303
bridge <group#> protocol ieee on page 304
clock [auto-correct-dst | no-auto-correct-dst] on page 305
clock set <time> <day> <month> <year> on page 306
clock timezone <text> on page 307
cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 310
crypto commands begin on page 313

line [console | telnet | ssh] <line-number> <ending number> on page 413

lldp [minimum-transmit-interval l reinitialization-delay l transmit-interval l ttl-multiplier] <numeric value> on page 415

logging commands begin on page 417

mac address-table aging-time <aging time> on page 431

mac address-table static <mac address> bridge <bridge id> interface <interface> on page 432

power-supply shutdown automatic on page 433

radius-server on page 436

radius-server host on page 438

route-map <map-name> [permit | deny] <sequence number> on page 439

router commands begin on page 440

service password-encryption on page 445

snmp-server commands begin on page 446

sntp server <address or hostname> version <1-3> on page 456

spanning tree commands begin on page 457

tacacs-server on page 466

thresholds [BES | CSS | DM | ES | LCV | LES | PCV | SEFS | SES | UAS] [15Min | 24Hr] <threshold count> on page 467

username <username> password <password> on page 469

aaa accounting commands *<level>* [*<listname>* | default] [none | stop-only] [group *<groupname>* | group tacacs+]

Use **aaa accounting commands** to set parameters for AAA accounting. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

<level>	Specifies the commands enable level. (1=unprivileged, 15 = privileged).
<listname>	Specifies the name of the list.
default	Uses the default accounting list.
none	Disables accounting.
stop-only	Records stop-only when service terminates.
group *<groupname>*	Uses the specified group of remote servers for accounting.
group tacacs+	Uses the TACACS+ server for accounting.

Default Values

By default, accounting is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example creates a list called myList and sets accounting for Level 1 commands at stop-only activities:

```
(config)#aaa accounting commands 1 myList stop-only group tacacs+
```

NOTE *To complete this command, Telnet must be applied to the lines. See Line (Telnet) Interface Config Command Set* on page 491 *for more detailed instructions.*

aaa accounting [suppress null-username]

Use the **aaa accounting suppress null-username** command to stop sending accounting records for usernames set to null. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

suppress	Refrain from sending accounting records for null usernames.

Default Values

By default, this command is disabled, which means the accounting records for null usernames are sent to the server.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following command causes the unit to refrain from sending accounting records for users with null usernames:

```
(config)#aaa accounting suppress null-username
```

aaa accounting update [newinfo | periodic *<minutes>*]

Use the **aaa accounting update** command to specify when accounting records are sent to the server. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

newinfo	Sends all new accounting records immediately.
periodic *<minutes>*	Periodically sends all accounting records to the server.

Default Values

By default, accounting records are sent every 5 minutes.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following command sets the unit to send accounting records every 600 minutes to the server:

```
(config)#aaa accounting update periodic 600
```

aaa authentication [banner | fail-message | password-prompt | username-prompt]

Use the **aaa authentication** command to control various features of the AAA subsystem authentication process. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

banner Sets the banner shown before user authentication is attempted. The banner can be multiple lines.

fail-message Sets the message shown if user authentication fails. The message can be multiple lines.

password-prompt Sets the prompt for the user's password. The prompt is a single line. Enclose the string in quotation marks.

username-prompt Sets the prompt for the user's name. The prompt is a single line. Enclose the string in quotation marks.

Default Values

banner	User Access Verification
fail-message	Authentication Failed
password-prompt	Password:
username-prompt	Username:

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following is a typical example of customizing the AAA authentication process:

```
(config)# aaa authentication banner #
Enter TEXT message. End with the character '#'.

User login authentication:#
(config)#

(config)#aaa authentication fail-message #
```

```
Enter TEXT message. End with the character '#'.
Authentication denied.#
(config)#

(config)#aaa authentication username-prompt “Enter Username:”

(config)#aaa authentication password-prompt “Enter Password:”
```

aaa authentication enable default [none | line | enable | group <*groupname*> | group radius | group tacacs+]

Use the **aaa authentication enable default** command to create (or change) the list of fallback methods used for privileged mode access authentication. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

none	Access automatically granted.
line	Uses the line password for authentication.
enable	Uses the enable password for authentication.
group <*groupname*>	Uses the specified group of remote servers for authentication.
group radius	Uses all defined RADIUS servers for authentication.
group tacacs+	Uses all defined TACACS+ servers for authentication.

Default Values

If there is no default methods list configured, the default behavior is to use the enable password for the unit. If there is no password configured, consoles are allowed access (this prevents a lock-out).

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.	The **group tacacs+** command was added.

Functional Notes

A user is authenticated by trying the list of methods from first to last until a method succeeds or fails. If a method is unable to complete, the next method is tried. The group falls through if the servers in the remote group cannot be found.

Note that enable access is a password-only process. The local-user database cannot be used, and the username given to any remote RADIUS server is **$enab15$**. The only list name allowed is **default**.

Usage Examples

The following example specifies using the line password as the first method for enable authentication and using the enable password as the second:

```
(config)#aaa authentication enable default line enable
```

aaa authentication login [<*listname*> | default] [none | line | enable | local | group <*groupname*> | group radius | group tacacs+]

Use the **aaa authentication login** command to create (or change) a named list with the ability to have a chain of fallback authentication methods for user authentication. Available methods for the fallback authentication methods are: no authentication (which grants login access without authentication), line password, enable password, local database, and defined group of servers. The defined server groups may be TACACS+ or RADIUS servers. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

<*listname*>	Specifies a named login list.
default	Specifies the default list used to authenticate users when no other list is assigned.
none	Access automatically granted.
line	Uses line password (Telnet 0-4 or console 0-1) for authentication.
enable	Uses enable password for authentication.
local	Uses local user database for authentication.
group <*groupname*>	Uses specified group of remote servers for authentication.
group radius	Uses defined RADIUS servers for authentication.
group tacacs+	Uses defined TACACS+ servers for authentication.

Default Values

The login list named **default** is the default list used to authenticate users when no other list is assigned.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.	The **group tacacs+** command was added.

Functional Notes

A user is authenticated by trying the list of methods from first to last until authentication succeeds or fails. If a method does not succeed or fail, the next method is tried. The local user database method falls through to the next method if the username does not appear in the database. The group method falls through if the servers in the remote group cannot be found. Refer to the command *radius-server* on page 436 or *tacacs-server* on page 466 for information on defining server groups.

Usage Examples

The following example creates a named list called myList and specifies using the local database as the first method, myGroup as the second method, and line password as the third method for login authentication:

```
(config)#aaa authentication login myList local group myGroup line
```

The following command sets the default authentication list for logins to use the local database as the first fallback method:

```
(config)#aaa authentication login default local
```

aaa authorization commands *<level>* [*<listname>* | default] [group *<groupname>* | group tacacs+ | if-authenticated | none]

Use **aaa authorization commands** to create (or change) a list of methods for user authorization. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

<level>	Specifies the commands enable level. (1=unprivileged, 15 = privileged).
<listname>	Specifies the name of the authorization list.
default	Specifies the default authorization list and applies it implicitly across all lines.
group *<groupname>*	Uses the specified group of remote servers for authorization.
group tacacs+	Uses all defined TACACS+ servers for authorization.
if-authenticated	Succeeds if user has authenticated.
none	Access automatically granted.

Default Values

The authorization list named **default** is the default list used to authorize commands when no other list is assigned to the line.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following command creates a list called **myList** to authorize unprivileged commands (which succeeds only if the user has been authenticated successfully):

```
(config)#aaa authorization commands 1 myList if-authenticated
```

The following command uses the default list to authorize privileged (level 15) commands against the defined TACACS+ servers:

```
(config)#aaa authorization commands 15 default group tacacs+
```

aaa authorization [config-command | console]

Use the **aaa authorization** to enable or disable authorization for configuration mode commands and for console mode. Use the **no** form of this command to return to the default setting. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

config-command	Enables authorization for configuration mode commands. Only level 1 (unprivileged) and level 15 (privileged) commands are supported.
console	Allows authorization to be applied to the console.

Default Values

By default, authorization for console is disabled. However, configuration mode commands are authorized by default.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables authorization of configuration mode commands:

```
(config)#aaa authorization config-command
```

The following example enables authorization of console commands:

```
(config)#aaa authorization console
```

aaa group server [radius | tacacs+] *<listname>*

Use the **aaa group server** command to group pre-defined RADIUS and TACACS+ servers into named lists. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

radius	Groups defined RADIUS servers.
tacacs+	Groups TACACS+ server.
<listname>	Specifies the name of the list.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.1	TACACS+ server support was added.

Functional Notes

Use the **radius-server** command to specify RADIUS servers before adding them to a group. Likewise, use the **tacacs-server** command to specify TACACS+ servers before adding them to a group. These commands enter a mode for adding individual servers to the named group. Refer to *Radius Group Command Set* on page 1169 or *TACACS+ Group Configuration Command Set* on page 1191 for more information.

The default group cannot be changed and includes all RADIUS servers in the order they were specified by the **radius-server** commands. The same is true of TACACS+ servers specified by the **tacacs-server** commands.

Usage Examples

The following example creates the named list **myServers** and enters the RADIUS group:

```
(config)#aaa group server radius myServers
(config-sg-radius)#
```

The following example creates the named list **myServers** and enters the TACACS+ group:

```
(config)#aaa group server tacacs myServers
(config-sg-tacacs+)#
```

aaa on

Use the **aaa on** command to activate the AAA subsystem. Use the **no** form of this command to deactivate AAA.

Syntax Description

No subcommands.

Default Values

By default, AAA is not activated.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

By default, the AAA subsystem is turned off and authentication follows the line technique (local, line, etc.). Once activated, the AAA lists override the methods specified in the line command.

Usage Examples

The following example activates the AAA subsystem:

```
(config)#aaa on
```

Technology Review

AAA stands for authentication, authorization, and accounting. The AOS AAA subsystem currently supports authentication. Authentication is the means by which a user is granted access to the device (router). For instance, a username/password is authenticated before the user can use the CLI. VPN clients can also verify username/password before getting access through the device.

There are several methods that can be used to authenticate a user:

NONE	Instant access
LINE-PASSWORD	Use the line password (telnet 0-4 or console 0-1)
ENABLE-PASSWORD	Use the enable password
LOCAL-USERS	Use the local-user database
GROUP <*groupname*>	Use a group of remote RADIUS servers

The AAA system allows users to create a named list of these methods to attempt in order (if one fails, it falls to the next one on the list). This named list is then attached to a portal (telnet 0-4 or console 0-1). When a user Telnets in or accesses the terminal, the AAA system uses the methods from the named list to authenticate the user.

The AAA system must be turned on to be active. By default it is off. Use the **aaa on** command to activate the AAA system.

If a portal is not explicitly assigned a named list, the name **default** is automatically assigned to it. Users can customize the **default** list just like any other list. If no **default** list is configured, the following default behavior applies (defaults are based on portal):

- Instant access (NONE) is assigned to the console using the **default** list (when the list has not been configured).
- The local-user database is used for Telnet sessions using the **default** list (when the list has not been configured).
- No access is granted for FTP access using the **default** list (when the list has not been configured).

Methods fail (and therefore cause the system to proceed to the next configured method) under the following circumstances:

- LINE and ENABLE passwords fall through if there are no LINE or ENABLE passwords configured.
- LOCAL-USERS fall through if the given user is not in the database.
- RADIUS server groups fall through if the given server(s) cannot be contacted on the network.

Example

For a default list defined with the order [LINE, ENABLE, LOCAL, and GROUP **mygroup**], the following statements are true:

- If there is no LINE password, the list falls through to the ENABLE password.
- If there is no ENABLE password, the AAA system prompts the user for a username and password for the local-user database.
- If the given user is not in the local list, the username and password are handed to the remote servers defined in **mygroup**.
- A failure at any point (password not matching) denies access.

If the AAA process falls through the list completely, system behavior is based on portal:

- Console access is granted if the process falls completely through (this prevents a lock-out condition).
- Telnet and FTP are denied access.

aaa processes *<threads>*

Use the **aaa processes** command to set the number of threads available to the AAA subsystem. Use the **no** form of this command to return to the default setting. For more detailed information on AAA functionality, refer to the *Technology Review* section of the command *aaa on* on page 296.

Syntax Description

<threads>	Specifies the number of threads available to the AAA subsystem. Range: 1 to 64.

Default Values

By default, this is set to 1 process.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Increasing this number may speed up simultaneous authentication at the cost of system resources (e.g., memory).

Usage Examples

The following example specifies five available threads for the AAA subsystem:

```
(config)#aaa processes 5
```

arp *<ip address> <mac address>* **arpa**

Use this command to enter static entries into the address resolution protocol (ARP) table.

Syntax Description

arpa	Sets the standard address resolution protocol for this interface.
<ip address>	Specifies the IP address.
<mac address>	Specifies the MAC address.

Default Values

The default for this command is **arpa**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 6.1	Command was extended to include NetVanta 2000 Series units.

Usage Examples

The following example enables standard ARP for the VLAN interface:

```
(config)#interface vlan 1
(config-interface-vlan 1)#arp 196.173.22.253 00:A0:C8:00:00:01 arpa
```

auto-config [filename *<name>* | restart | retry-count *<number>*| server *<name or address>*]

Use the **auto-config** command to enable the automatic self-configuration feature in ADTRAN OS. Use the **no** form of this command to halt the Auto-Config process. For more detailed information on auto-config, see the Auto-Config Configuration Guide on the documentation CD, PN 61200560L1-29.2.

NOTE *Refer to the* ***Auto-Config Configuration Guide*** *(61200560L1-29.2) for more information on this command. This document is located on the* ***ADTRAN OS Documentation*** *CD provided with your unit*

Syntax Description

filename *<name>*	Specifies the configuration filename to download.
restart	Restarts auto-config parameters.
retry-count *<number>*	Specifies the maximum number of retries. Range: 0 to 1000.
server *<name or address>*	Specifies the IP address or host name of TFTP Server from which to download.

Default Values

By default, auto-config is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following command enables **auto-config**:

(config)#**auto-config**

NOTE *Disabling and re-enabling* ***auto-config*** *restarts the download process.*

The following command specifies the name of the file to download:
(config)#**auto-config filename myConfig**

The following command restarts the auto-config process:
(config)#**auto-config restart**

The following command sets the number of retries when downloading a configuration file to 100:
(config)#**auto-config retry-count 100**

The following command specifies the TFTP server IP address from which to download the configuration file:
(config)#**auto-config server 192.33.5.99**

The following command specifies the TFTP server hostname from which to download the configuration file:
(config)#**auto-config server myHost**

banner [exec | login | motd] *<character> <message> <character>*

Use the **banner** command to specify messages to be displayed in certain situations. Use the **no** form of this command to delete a previously configured banner.

Syntax Description

exec	Creates a message to be displayed when any exec-level process takes place.
login	Creates a message to be displayed before the username and password login prompts.
motd	Creates a message-of-the-day (MOTD) banner.
<*character*>	Specifies the banner text delimiter character. Press **Enter** after the delimiter to begin input of banner text.
<*message*>	Specifies the text message you wish to display. End with the character that you specified as your delimiter.

Default Values

By default, no banners are configured.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Banners appear in the following order (if configured):

- MOTD banner appears at initial connection.
- Login banner follows the MOTD banner.
- Exec banner appears after successful login.

Usage Examples

The following example configures the system to display a message of the day:

```
(config)#banner motd *The system will be shut down today from 7PM to 11PM*
```

boot system flash *<filename>* [no-backup | *<backup filename>*]

Use the **boot system flash** command to specify the system image loaded at startup.

Syntax Description

<filename>	Specifies the filename (located in flash memory) of the image (filenames are case-sensitive) - image files should have a .biz extension
no-backup	Specifies that no backup image is to be saved to the system.
<backup filename>	Specifies a name for the backup image.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Detailed instructions for upgrading the AOS and loading files into flash memory are found on the ***ADTRAN OS Documentation*** CD.

bridge *<group#>* protocol ieee

The **bridge protocol ieee** command configures a bridge group for the IEEE Spanning-Tree Protocol. Use the **no** form of this command (with the appropriate arguments) to delete this setting.

Syntax Description

<group#>	Specifies a bridge group number (range: 1 to 255).
ieee	Specifies IEEE 802.1 Ethernet spanning-tree protocol.

Default Values

By default, all configured bridge interfaces implement **ieee** spanning-tree protocol.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example deletes the bridge protocol setting for bridge-group 17:

```
(config)#no bridge 17 protocol ieee
```

clock [auto-correct-dst | no-auto-correct-dst]

The **clock auto-correct-dst** command allows the unit to automatically correct for Daylight Saving Time (DST). Use the **clock no-auto-correct-dst** command to disable this feature.

Syntax Description

auto-correct-DST	Configures the unit to automatically correct for DST.
no-auto-correct-DST	Disables DST correction.

Default Values

By default DST correction takes place automatically.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was added to the Global command set.

Functional Notes

Depending on the **clock timezone** chosen (see *clock timezone <text>* on page 307 for more information) one-hour DST correction may be enabled automatically. You may override this default using this command.

Usage Examples

The following example allows for automatic DST correction:

```
(config)#clock auto-correct-dst
```

The following example overrides the one-hour offset for DST:

```
(config)#clock no-auto-correct-dst
```

clock set *<time> <day> <month> <year>*

Use the **clock set** command to configure the system software clock. For the command to be valid, all fields must be entered. Refer to the **Usage Example** below for an example.

Syntax Description

<time>	Sets the time (in 24-hour format) of the system software clock in the format HH:MM:SS (hours:minutes:seconds).
<day>	Sets the current day of the month (valid range: 1 to 31).
<month>	Sets the current month (valid range: January to December). You need only enter enough characters to make the entry unique. This entry is not case-sensitive.
<year>	Sets the current year (valid range: 2000 to 2100).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command was added to the Global command set.

Usage Examples

The following example sets the system software clock for 3:42 pm, August 22 2004:

```
(config)#clock set 15:42:00 22 Au 2004
```

clock timezone *<text>*

The **clock timezone** command sets the unit's internal clock to the timezone of your choice. This setting is based on the difference in time (in hours) between Greenwich Mean Time (GMT) or Central Standard Time (CST) and the timezone for which you are setting up the unit. Use the **no** form of this command to disable this feature.

Syntax Description

Subcommands are specified in the *Functional Notes* section for this command.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

NOTE *Depending on the* ***clock timezone*** *chosen, one-hour Daylight Savings Time (DST) correction may be enabled automatically. See clock [auto-correct-dst | no-auto-correct-dst]* on page 305 *for more information.*

Functional Notes

The following list shows sample cities and their timezone codes.

```
clock timezone +1-Amsterdam
clock timezone +1-Belgrade
clock timezone +1-Brussels
clock timezone +1-Sarajevo
clock timezone +1-West-Africa
clock timezone +10-Brisbane
clock timezone +10-Canberra
clock timezone +10-Guam
clock timezone +10-Hobart
clock timezone +10-Vladivostok
clock timezone +11
clock timezone +12-Auckland
clock timezone +12-Fiji
clock timezone +13
clock timezone +2-Athens
clock timezone +2-Bucharest
clock timezone +2-Cairo
clock timezone +2-Harare
clock timezone +2-Helsinki
clock timezone +2-Jerusalem
clock timezone +3-Baghdad
clock timezone +3-Kuwait
clock timezone +3-Moscow
clock timezone +3-Nairobi
clock timezone +3:30
clock timezone +4-Abu-Dhabi
clock timezone +4-Baku
clock timezone +4:30
clock timezone +5-Ekaterinburg
clock timezone +5-Islamabad
clock timezone +5:30
clock timezone +5:45
clock timezone +6-Almaty
clock timezone +6-Astana
clock timezone +6-Sri-Jay
clock timezone +6:30
clock timezone +7-Bangkok
clock timezone +7-Kranoyarsk
clock timezone +8-Bejing
clock timezone +8-Irkutsk
clock timezone +8-Kuala-Lumpur
clock timezone +8-Perth
clock timezone +8-Taipei
clock timezone +9-Osaka
clock timezone +9-Seoul
clock timezone +9-Yakutsk
clock timezone +9:30-Adelaide
clock timezone +9:30-Darwin
clock timezone -1-Azores
clock timezone -1-Cape-Verde
clock timezone -10
clock timezone -11
clock timezone -12
clock timezone -2
clock timezone -3-Brasilia
clock timezone -3-Buenos-Aires
clock timezone -3-Greenland
clock timezone -3:30
clock timezone -4-Atlantic-Time
clock timezone -4-Caracus
clock timezone -4-Santiago
clock timezone -5
clock timezone -5-Bogota
clock timezone -5-Eastern-Time
clock timezone -6-Central-America
clock timezone -6-Central-Time
clock timezone -6-Mexico-City
clock timezone -6-Saskatchewan
clock timezone -7-Arizona
clock timezone -7-Mountain-Time
clock timezone -8
clock timezone -9
clock timezone GMT-Casablanca
clock timezone GMT-Dublin
```

Usage Examples

The following example sets the timezone for Santiago, Chile.

```
>enable
(config)#clock timezone -4-Santiago
```

cross-connect *<#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port>*

Use the **cross-connect** command to create a cross-connect map from a created TDM group on an interface to a virtual interface.

> CAUTION *Changing* ***cross-connect*** *settings could potentially result in service interruption.*

Syntax Description

<#>	Identifies the cross-connect using a number descriptor or label for (useful in systems that allow multiple cross-connects).
<from interface>	Specifies the interface (physical or virtual) on one end of the cross-connect. Enter **cross-connect 1 ?** for a list of valid interfaces.
<slot/port>	Used when a physical interface is specified in the *<from interface>* subcommand (For example: specifying the T1 port of a T1 module would be **t1 1/1**).
<tdm-group#>	Specifies which configured TDM group to use for this cross-connect. This subcommand only applies to T1 physical interfaces.
<to interface>	Specifies the virtual interface on the other end of the cross-connect. Use the **?** to display a list of valid interfaces.
<slot/port>	Used when a physical interface is specified in the *<to interface>* subcommand. (For example, specifying the primary T1 port of a T1 module would be **t1 1/1**).

Default Values

By default, there are no configured cross-connects.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the E1 interface.

Functional Notes

Cross-connects provide the mechanism for connecting a configured virtual (layer 2) endpoint with a physical (layer 1) interface. Supported layer 2 protocols include Frame Relay and point-to-point protocol (PPP).

Usage Examples

The following example creates a Frame Relay endpoint and connects it to the T1 1/1 physical interface:

1. Create the Frame Relay virtual endpoint and set the signaling method:

```
(config)# interface frame-relay 1
(config-fr 1)# frame-relay lmi-type cisco
```

2. Create the sub-interface and configure the PVC parameters (including DLCI and IP address):

```
(config-fr 1)# interface fr 1.1
(config-fr 1.1)# frame-relay interface-dlci 17
(config-fr 1.1)# ip address 168.125.33.252 255.255.255.252
```

3. Create the TDM group of 12 DS0s (64K) on the T1 physical interface:
(THIS STEP IS ONLY VALID FOR T1 INTERFACES.)

```
(config)# interface t1 1/1
(config-t1 1/1)# tdm-group 1 timeslots 1-12 speed 64
(config-t1 1/1)# exit
```

4. Connect the Frame Relay sub-interface with port T1 1/1:

```
(config)# cross-connect 1 t1 1/1 1 fr 1
```

Technology Review

Creating an endpoint that uses a layer 2 protocol (such as Frame Relay) is generally a four-step process:

Step 1:

Create the Frame Relay virtual endpoint (using the **interface frame-relay** command) and set the signaling method (using the **frame-relay lmi-type** command). Also included in the Frame Relay virtual endpoint are all the applicable Frame Relay timers logging thresholds, encapsulation types, etc. Generally, most Frame Relay virtual interface parameters should be left at their default state. For example, the following creates a Frame Relay interface labeled **7** and sets the signaling method to **ansi**.

```
(config)# interface frame-relay 7
(config-fr 7)# frame-relay lmi-type ansi
```

Step 2:

Create the sub-interface and configure the PVC parameters. Using the sub-interface, apply access policies to the interface, create bridging interfaces, configure dial-backup, assign an IP address, and set the PVC data-link control identifier (DLCI). For example, the following creates a Frame Relay sub-interface labeled **22,** sets the DLCI to **30,** and assigns an IP address of **193.44.69.253** to the interface.

```
(config-fr 7)# interface fr 7.22
(config-fr 7.22)# frame-relay interface-dlci 30
(config-fr 7.22)# ip address 193.44.69.253 255.255.255.252
```

Step 3: (VALID ONLY FOR T1 INTERFACES)

Specify the group of DS0s used for signaling on the T1 interface by creating a TDM group. Group any number of contiguous DS0s together to create a data pipe for layer 2 signaling. Also use the **tdm-group** command to specify the per-DS0 signaling rate on the interface. For example, the following creates a TDM group labeled **9** containing 20 DS0s (each DS0 having a data rate of 56 kbps).

```
(config)# interface t1 1/1
(config-t1 1/1)# tdm-group 9 timeslots 1-20 speed 56
(config-t1 1/1)# exit
```

Step 4:

Make the association between the layer 2 endpoint and the physical interface using the **cross-connect** command. Supported layer 2 protocols include Frame Relay and point-to-point protocol (PPP). For example, the following creates a cross-connect (labeled **5**) to make an association between the Frame Relay virtual interface (**fr 7**) and the TDM group configured on interface t1 1/1 (**tdm-group 9**).

```
(config)# cross-connect 5 t1 1/1 9 fr 7
```

crypto ca authenticate *<name>*

Use the **crypto ca authenticate** command to initiate CA authentication procedures.

Syntax Description

<name>	Specifies a CA profile using an alphanumeric string up to 32 characters.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The type of authentication procedure is based on the **enrollment** command and its settings. Refer to *enrollment terminal* on page 1032 and *enrollment url <url>* on page 1033 for more information. When **enrollment** is set to **terminal**, the CA authentication process is done manually, as shown in the following *Usage Examples*.

Usage Examples

The following example initiates the CA authentication process:

```
(config)#crypto ca authenticate testCAprofile
Enter the base 64 encoded CA certificate. End with two consecutive carriage returns or the word "quit" on
a line by itself:
-----BEGIN X509 CERTIFICATE-----
MIIDEDCCAs6gAwIBAgICAXIwCwYHKoZIzjgEAwUAMFoxCzAJBgNVBAYTAkZJMSQw
IgYDVQQKExtTU0ggQ29tbXVuaWNhdGlvbnMgU2VjdXJpdHkxETAPBgNVBAsTCFdl
YiB0ZXN0MRIwEAYDVQQDEwlUZXN0IENBIDQwHhcNMDMwMTA5MTYyNTE1WhcNMDMx
MjMxMjM1OTU5WjBaMQswCQYDVQQGEwJGSTEkMCIGA1UEChMbU1NIIENvbW11bmlj
YXRpb25zIFNlY3VyaXR5MREwDwYDVQQLEwhXZWIgdGVzdDESMBAGA1UEAxMJVGVz
dCBDQSA0MIIBtzCCASsGByqGSM44BAEwggEeAoGBAPTo+NdCWh87hOSnuZ7dUL07
twjZZwY3beLHnDsERhfN8XoOZZcffulKc/lqTrYiu7M5yPJsXQ3u8dbCb6RWFU0A
T5Nd7/4cNn/hCmhbeb6xqsNZUsOcTZJxvClq8thkNo+gXg5bw0fiElgxZ/lEbFWL
UzeO8KgM4izkq0CrGtaFAhUA2+ja4RgbbgTgJk+qTXAxicG/8JMCgYBZvcPMO2/Y
```

```
Zc2sXYyrBPtv6k2ZGGYqXAUZ98/txm37JwQGafygePJ/64oeisVeDcLf2FTjveex
W5saydjSK00jXjreRZcJFEDmfRhUtWR8K8tm8mEnB3eg9n09lkWibIjihHn7n5MF
tBBAdbRHyctsr3DyofnieTt3DY78MDsNbgOBhQACgYEA6EKDS2IxrdMsogHfVvob
PkDSv2FjOsP5Tomc/tf9jvvuf6+vj9XTw+uAg1BU9/TyjGzAtnRrCvOUkTYoVxRY
vdDOi3GR2RcyNVdGrhYXWY1I5XuB5+NWij8VUQOgfXsJgbEMvPemECeYwQ4ASdhD
vw0E8NI2AEkJXsCAvYfXWzujIzAhMAsGA1UdDwQEAwIBhjASBgNVHRMBAf8ECDAG
AQH/AgEyMAsGByqGSM44BAMFAAMvADAsAhRa0ao0FbRQeWCc2oC24OZ1YZi8egIU
IZhxKAclhXksZHvOj+yIld5x0ec=
-----END X509 CERTIFICATE-----
quit

Hash: 4e904504dc4e5b95e08129430e2a0b97ceef0ad1394f905b42df2dfb8f751be0244a711bb0
6eddaa2f07dd640c187f14c16fa0bed28e038b28b6741a880539d6ed06a68b7e324bfdde6f3d0b17
83d94e58fd4943f5988a7a0f27f6b6b932dc0410378247160752853858dbe7a1951245cfb14b109e
ffc430e177623720de56f4

* Do you accept this certificate? [y]y
```

crypto ca certificate chain *<name>*

Use the **crypto ca certificate chain** command to enter the Certificate Configuration for the specified CA. Refer to *Certificate Configuration Command Set* on page 1039 for more information.

Syntax Description

<name>	Specifies a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Typically used only in the **running-config** and **startup-config** to restore certificates.

Usage Examples

The following example enters the Certificate Configuration mode for the CA profile **MyProfile**:

```
(config)#crypto ca certificate chain MyProfile
```

crypto ca enroll *<name>*

Use the **crypto ca enroll** command to begin CA enrollment procedures.

Syntax Description

<name>	Specifies a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The type of enrollment procedure is based on the **enrollment** command and its settings. Refer to *enrollment terminal* on page 1032 and *enrollment url <url>* on page 1033 for more information. This command initiates a dialog that is used to fill in the parameters that make up an enrollment request to be forwarded to a certificate authority. Note that some of the parameters (such as IP address) may be filled in using the values supplied in the **crypto ca profile** (in which case, the enrollment dialog will not prompt for those parameters). Once all required parameters are defined using the dialog, this command assembles them into an enrollment request to be sent to a certificate authority (including the generation of public and private keys). Refer to *crypto ca profile <name>* on page 321 for more information.

If **enrollment** is set to **terminal**, you may view the request on the terminal screen.

If **enrollment** is set to **url**, the request is sent automatically to the certificate authority using the URL specified by the **enrollment url** command.

Usage Examples

The following example shows a typical enrollment dialog:

```
(config)#crypto ca enroll MyProfile

**** Press CTRL+C to exit enrollment request dialog. ****
* Enter signature algorithm (RSA or DSS) [rsa]:rsa
* Enter the modulus length to use [512]:1024
* Enter the subject name as an X.500 (LDAP) DN:CN=Router,C=US,L=Huntsville,S=AL
  --The subject name in the certificate will be CN=CN=Router,C=US,L=Huntsville,S=AL.
* Include an IP address in the subject name [n]:y
* Enter IP address or name of interface to use:10.200.1.45
* Include fully qualified domain name [n]:y
* Enter the fully qualified domain name to use:FullyQualifiedDomainName
* Include an email address [n]:y
* Enter the email address to use:myEmail@adtran.commyemail@email.com
Generating request (including keys)....
```

crypto ca import *<name>* certificate

Use the **crypto ca import certificate** command to import a certificate manually via the console terminal.

Syntax Description

<name>	Specifies a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Puts CLI in mode where the certificate can be entered manually. Enter **quit** and a carriage return (or simply enter two consecutive carriage returns) to exit this mode. Abort this mode by pressing **Ctrl-C**. This command only applies if the **enrollment** command is set to **terminal**. Refer to *enrollment terminal* on page 1032.

Usage Examples

The following example imports a certificate via the console terminal:

```
(config)#crypto ca import MyProfile certificate
Enter the PM-encoded certificate. End with two consecutive
carriage returns or the word “quit” on a line by itself:
-----BEGIN CERTIFICATE-----
MIIDWTCCAwOgAwIBAgIKFLCsOgAAAAAAtjANBgkqhkiG9w0BAQUFADBjMQswCQYD
VQQGEwJVUzEQMA4GA1UECBMHQUxBQkFNQTETMBEGA1UEBxMKSHVudHN2aWxsZTEa
MBgGA1UEChMRQWR0cmFuVGVjaFN1cHBvcnQxETAPBgNVBAMTCHRzcm91dGVyMB4X
DTAzMDYyNTE0MTM1NVoXDTAzMTIwNjE0NDkxM1owJDEPMA0GA1UEChMGYWR0cmFu
MREwDwYDVQQDEwhNeVJvdXRlcjBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQClUKqs
fbTalej5m9gk2DMsbC9df3TilBz+7nRx3ZzGw75AQsqEMYeBY5aWi62W59jmxGSE
WX+E8EwBVbZ6JKk5AgMBAAGjggHWMIIB0jAXBgNVHREEEDAOhwQKCgoKggZNeUZx
ZG4wHQYDVR0OBBYEFJAvBRIjx1PROnkZ4v0D89yB1eErMIGcBgNVHSMEgZQwgZGA
FHGwIRAr11495MgrLNPiLzjvrb4JoWekZTBjMQswCQYDVQQGEwJVUzEQMA4GA1UE
CBMHQUxBQkFNQTETMBEGA1UEBxMKSHVudHN2aWxsZTEaMBgGA1UEChMRQWR0cmFu
```

```
VGVjaFN1cHBvcnQxETAPBgNVBAMTCHRzcm91dGVyghAZql7OwISgsUhfaSeGh0Ot
MGkGA1UdHwRiMGAwLaAroCmGJ2h0dHA6Ly90c3JvdXRlci9DZXJ0RW5yb2xsL3Rz
cm91dGVyLmNybDAvoC2gK4YpZmlsZTovL1xcdHNyb3V0ZXJcQ2VydEVucm9sbFx0
c3JvdXRlci5jcmwwgY0GCCsGAQUFBwEBBIGAMH4wPAYIKwYBBQUHMAKGMGh0dHA6
Ly90c3JvdXRlci9DZXJ0RW5yb2xsL3Rzcm91dGVyX3Rzcm91dGVyLmNydDA+Bggr
BgEFBQcwAoYyZmlsZTovL1xcdHNyb3V0ZXJcQ2VydEVucm9sbFx0c3JvdXRlcl90
c3JvdXRlci5jcnQwDQYJKoZIhvcNAQEFBQADQQBSGD4JbGJGk53qvyy0xXVoMQvy
U8xNjUdvWqjgFOI+2m8ZYJcfhnt11rbP2f3Wm9TpjLe1WuBNxmpNjC9A2ab0
-----END CERTIFICATE-----

Success!
```

crypto ca import *<name>* crl

Use the **crypto ca import crl** command to import a CRL manually via the console terminal.

Syntax Description

<name>	Specifies a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Puts CLI in a mode where the CRL can be entered manually. Enter **quit** and a carriage return (or simply enter two consecutive carriage returns) to exit this mode. This command only applies if the **enrollment** command is set to **terminal**. Refer to *enrollment terminal* on page 1032.

Usage Examples

The following allows you to manually paste in the CA’s CRL:

```
(config)#crypto ca import MyProfile crl
```

crypto ca profile *<name>*

Use the **crypto ca profile** command to define a CA and to enter the CA Profile Configuration. Refer to *CA Profile Configuration Command Set* on page 1028 for more information.

Syntax Description

<name>	Creates a CA profile using an alphanumeric string (up to 32 characters).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Use this to specify the type of enrollment, as well as enrollment request parameters. Refer to the *Functional Notes* of the command *crypto ca enroll <name>* on page 316 for more information.

Usage Examples

The following example creates the CA profile called **MyProfile** and enters the CA Profile Configuration for that certificate authority:

```
(config)#crypto ca profile MyProfile
Configuring New CA Profile MyProfile.
(ca-profile)#
```

crypto ike

Use the **crypto ike** command to define the system-level local ID for IKE negotiations and to enter the IKE Client or IKE Policy command sets.

Variations of this command include the following:

crypto ike client configuration pool *<poolname>*

crypto ike local-id address

crypto ike policy *<policy priority>*

Syntax Description

client configuration pool *<poolname>*	Creates a local pool named the *<poolname>* of your choice and enters the IKE Client. Clients that connect via an IKE policy that specifies this pool-name will be assigned values from this pool. Refer to the section *IKE Client Command Set* on page 1063 for more information.
local-id address	Sets the local ID during IKE negotiation to be the IP address of the interface from which the traffic exits. This setting can be overridden on a per-policy basis using the **local-id** command in the IKE Policy (refer to *local-id [address | asn1-dn | fqdn | user-fqdn] <ipaddress or name>* on page 1080 for more information).
policy *<policy priority>*	Creates an IKE policy with the *<policy priority>* of your choice and enters the IKE Policy. Refer to *IKE Policy Command Set* on page 1073 for more information.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example creates an IKE policy with a policy priority setting of 1 and enters the IKE Policy for that policy:

```
(config)#crypto ike policy 1
```

Technology Review

The following example configures an AOS product for VPN using IKE aggressive mode with pre-shared keys. The AOS product can be set to initiate IKE negotiation in main mode or aggressive mode. The product can be set to respond to IKE negotiation in main mode, aggressive mode, or any mode. In this example, the device is configured to initiate in aggressive mode and to respond to any mode.

This example assumes that the AOS product has been configured with a WAN IP address of 63.97.45.57 on interface **ppp 1** and a LAN IP address of 10.10.10.254 on interface **ethernet 0/1**. The peer private IP Subnet is 10.10.20.0.

For more detailed information on VPN configuration, refer to the technical support note *VPN* Configuration Guide located on the ***ADTRAN OS Documentation*** CD provided with your unit.

Step 1:

Enter the Global configuration mode (i.e., config terminal mode).

```
>enable
#configure terminal
```

Step 2:

Enable VPN support using the **ip crypto** command. This command allows crypto maps to be applied to interfaces, and enables the IKE server to listen for IKE negotiation sessions on UDP port 500.

```
(config)#ip crypto
```

Step 3:

Set the local ID. During IKE negotiation, local IDs are exchanged between the local device and the peer device. In the AOS, the default setting for all local IDs are configured by the **crypto ike local-id** command. The default setting is for all local IDs to be the IPv4 address of the interface over which the IKE negotiation is occurring. In the future, a unique system-wide hostname or fully qualified domain name could be used for all IKE negotiation.

```
(config)#crypto ike local-id address
```

Step 4:

Create IKE policy. In order to use IKE negotiation, an IKE policy must be created. Within the system, a list of IKE policies is maintained. Each IKE policy is given a priority number in the system. That priority number defines the position of that IKE policy within the system list. When IKE negotiation is needed, the system searches through the list, starting with the policy with priority of 1, looking for a match to the peer IP address.

An individual IKE policy can override the system local ID setting by having the **local-id** command specified in the IKE policy definition. This command in the IKE policy is used to specify the type of local ID and the local ID data. The type can be of IPv4 address, fully qualified domain name, or user-specified fully qualified domain name.

An IKE policy may specify one or more peer IP addresses that will be allowed to connect to this system. To specify multiple unique peer IP addresses, the **peer A.B.C.D** command is used multiple times within a single IKE policy. To specify that all possible peers can use a default IKE policy, the **peer any** command is given instead of the **peer A.B.C.D** command inside of the IKE policy. The policy with the **peer any** command specified will match to any peer IP address (and therefore should be given the highest numerical priority number). This will make the policy the last one to be compared against during IKE negotiation.

```
(config)#crypto ike policy 10
(config-ike)#no local-id
(config-ike)#peer 63.105.15.129
(config-ike)#initiate aggressive
(config-ike)#respond anymode
(config-ike)#attribute 10
(config-ike-attribute)#encryption 3des
(config-ike-attribute)#hash sha
(config-ike-attribute)#authentication pre-share
(config-ike-attribute)#group 1
(config-ike-attribute)#lifetime 86400
```

Step 5:

Define the remote ID settings. The **crypto ike remote-id** command is used to define the remote ID for a peer connecting to the system, specify the preshared-key associated with the specific remote ID, and (optionally) determine that the peer matching this remote ID should not use mode config (by using the **no-mode-config** keyword). Refer to *crypto ike remote-id* on page 326 for more information.

```
(config)#crypto ike remote-id address 63.105.15.129 preshared-key mysecret123
```

Step 6:

Define the transform-set. A transform set defines the encryption and/or authentication algorithms to be used to secure the data transmitted over the VPN tunnel. Multiple transform sets may be defined in a system. Once a transform set is defined, many different crypto maps within the system can reference it. In this example, a transform set named **highly_secure** has been created. This transform set defines ESP with authentication implemented using 3DES encryption and SHA1 authentication.

```
(config)#crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac
(cfg-crypto-trans)#mode tunnel
```

Step 7:

Define an IP access list. An extended access control list is used to specify which traffic needs to be sent securely over the VPN tunnel. The entries in the list are defined with respect to the local system. The source IP address will be the source of the traffic to be encrypted. The destination IP address will be the receiver of the data on the other side of the VPN tunnel.

```
(config)#ip access-list extended corporate_traffic
(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 log deny ip any any
```

Step 8:

Create crypto map. A crypto map is used to define a set of encryption schemes to be used for a given interface. A crypto map entry has a unique index within the crypto map set. The crypto map entry will specify whether IKE is used to generate encryption keys or if manually specified keys will be used. The crypto map entry will also specify who will be terminating the VPN tunnel, as well as which transform set or sets will be used to encrypt and/or authenticate the traffic on that VPN tunnel. It also specifies the lifetime of all created IPSec security associations.

```
(config)#crypto map corporate_vpn 1 ipsec-ike
(config-crypto-map)#match address corporate_traffic
(config-crypto-map)#set peer 63.105.15.129
(config-crypto-map)#set transform-set highly_secure
(config-crypto-map)#set security-association lifetime kilobytes 8000
(config-crypto-map)#set security-association lifetime seconds 28800
(config-crypto-map)#no set pfs
```

Step 9:

Configure a public interface. This process includes configuring the IP address for the interface and applying the appropriate crypto map to the interface. Crypto maps are applied to the interface on which encrypted traffic will be transmitted.

```
(config)#interface ppp 1
(config-ppp 1)#ip address 63.97.45.57 255.255.255.248
(config-ppp 1)#crypto map corporate_vpn
(config-ppp 1)#no shutdown
```

Step 10:

Configure a private interface. This process allows all traffic destined for the VPN tunnel to be routed to the appropriate gateway.

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ip address 10.10.10.254 255.255.255.0
(config-eth 0/1)#no shutdown
(config-eth 0/1)#exit
```

crypto ike remote-id

Use the **crypto ike remote-id** command to specify the remote ID and to associate a pre-shared key with the remote ID.

> *For VPN configuration example scripts, refer to the technical support note* ***VPN Configuration Guide*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

address *<IPv4 address>*	Specifies a remote ID of IPv4 type.
any	Wildcard that allows any remote ID (type and value).
asn1-dn *<name>*	Specifies an abstract syntax notation distinguished name as the remote ID (enter this value in LDAP format).
fqdn *<fqdn>*	Specifies a fully qualified domain name (e.g., adtran.com) as the remote ID.
user-fqdn *<fqdn>*	Specifies a user fully qualified domain name or email address (e.g., user1@adtran.com) as the remote ID.
preshared-key *<keyname>*	Associates a preshared key with this remote ID.
no-mode-config	Optional. keyword used to specify that the peer matching this remote ID should not use mode config.
no-xauth	Optional. Keyword used to specify that the peer matching this remote ID should not use xauth.
nat-t [v1 l v2] [allow l force l disable]	Optional. Keyword that denotes whether peers matching this remote ID should allow, disable, or force NAT traversal versions 1 and 2.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include the **any**, **asn1-dn**, and **no-xauth** subcommands.
Release 7.1	Command was expanded to include NAT traversal commands.

Functional Notes

The **fqdn** and **user-fqdn** <*fqdn*> line can include wildcard characters. The wildcard characters are "*****" for a 0 or more character match and "?" for a single character match. Currently, the "?" cannot be set up using the CLI, but it can be transferred to the unit via the startup-config.

Example for **user-fqdn**:

john*@domain.com
will match:
johndoe@domain.com
johnjohn@adtran.comjohnjohn@myemail.com
john@adtran.comjohn@myemail.com

Example for **fqdn**:

***.domain.com**
will match:
www.domain.com
ftp.domain.com
one.www.domain.com

The **address** remote ID can be in the form of a single host address or in the form of an IP address wildcard.

Example for **address** type:

crypto ike remote id address 10.10.10.0 0.0.0.255
will match:

10.10.10.1
10.10.10.2
and all IP addresses in the form of 10.10.10.X (where X is 0 to 255)

The **asn1-dn** <*name*> line can include wildcard characters. The wildcard characters are "*" for a 0 or more character match and "?" for a single character match. Currently, the "?" cannot be set up using the CLI, but it can be transferred to the unit via the startup-config.

Example for typical **asn1-dn** format with no wildcards:

crypto ike remote-id asn1-dn "CN=MyRouter, C=US, S=ALCA, L=Huntsville, O=Adtran, OU=TechSupport"
(matches only remote ID strings with all fields exactly the same)

Example for typical **asn1-dn** format with wildcards used to match a string within a field:

crypto ike remote-id asn1-dn "CN=*, C=*, S=*, L=*, O=*, OU=*"
(matches any asn1-dn remote ID string from a peer)

Example for typical **asn1-dn** format with wildcards used to match a portion of the remote ID:

crypto ike remote-id asn1-dn "CN=*, C=US, S=ALCA, L=Huntsville, O=Adtran, OU=*"
(matches any remote ID string with the same values for the C, S, L, and O fields, and any values in the CN and OU fields)

Example for typical **asn1-dn** format with wildcards used to match a portion of a field:

crypto ike remote-id asn1-dn "CN=My*, C=US, S=ALCA, L=Huntsville, O=Adtran, OU=TechSupport"
(matches remote ID strings with all fields exactly the same, but with any CN field beginning with “My”)

Usage Examples

The following example assigns a remote ID of 63.97.45.57 and associates the preshared key **mysecret** with the remote ID:

```
(config)#crypto ike remote-id address 63.97.45.57 preshared-key mysecret
```

crypto ipsec transform-set *<setname> <parameters>*

Use the **crypto ipsec transform-set** command to define the transform configuration for securing data (e.g., esp-3des, esp-sha-hmac, etc.). The transform set is then assigned to a crypto map using the map's **set transform-set** command. Refer to *set transform-set <setname1 - setname6>* on page 1051.

> NOTE *For VPN configuration example scripts, refer to the technical support note **VPN Configuration Guide** located on the **ADTRAN OS Documentation** CD provided with your unit.*

Syntax Description

<setname> Assigns a name to the transform set you are about to define.

<parameters> Assigns a combination of up to three security algorithms. This field is a valid combination of the following:

- ah-md5-hmac, ah-sha-hmac
- esp-des, esp-3des, esp-aes-128-cbc, esp-aes-192-cbc, esp-aes-256-cbc, esp-null
- esp-md5-hmac, esp-sha-hmac

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, and 4000 and Total Access 900 Series units.

Command History

Release 4.1 Command was introduced.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms.

If no transform set is configured for a crypto map, the entry is incomplete and will have no effect on the system.

Usage Examples

The following example first creates a transform set (**Set1**) consisting of two security algorithms (up to three may be defined), and then assigns the transform set to a crypto map (**Map1**):

```
(config)#crypto ipsec transform-set Set1 esp-3des esp-sha-hmac
(cfg-crypto-trans)#exit

(config)#crypto map Map1 1 ipsec-ike
(config-crypto-map)#set transform-set Set1
```

crypto map

Use the **crypto map** command to define crypto map names and numbers and to enter the associated mode (either Crypto Map IKE or Crypto Map Manual).

Variations of this command include the following:

crypto map <*mapname*> <*mapindex*> **ipsec-ike**
crypto map <*mapname*> <*mapindex*> **ipsec-manual**

> NOTE *For VPN configuration example scripts, refer to the technical support note **VPN Configuration Guide** located on the **ADTRAN OS Documentation** CD provided with your unit.*

Syntax Description

<*mapname*>	Names the crypto map. You can assign the same name to multiple crypto maps, as long as the map index numbers are unique.
<*mapindex*>	Assigns a crypto map sequence number.
ipsec-ike	Specifies the Crypto Map IKE (refer to *Crypto Map IKE Command Set* on page 1043). This supports IPSec entries that will use IKE to negotiate keys.
ipsec-manual	Specifies the Crypto Map Manual (refer to *Crypto Map Manual Command Set* on page 1052). This supports manually configured IPSec entries.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms (refer to *crypto ipsec transform-set <setname> <parameters>* on page 329).

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list is assigned to the crypto map using the **match address** command (refer to *ike-policy <policy number>* on page 1045).

If no transform set or access list is configured for a crypto map, the entry is incomplete and will have no effect on the system.

When you apply a crypto map to an interface (using the **crypto map** command within the interface's mode), you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps that share the same name but have different map index numbers.

Usage Examples

The following example creates a new IPSec IKE crypto map called **testMap** with a map index of **10**:

```
(config)#crypto map testMap 10 ipsec-ike
(config-crypto-map)#
```

Technology Review

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: **ipsec-manual** and **ipsec-ike**. Each entry is given an index, which is used to sort the ordered list. When a nonsecured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the nonsecured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable security association (SA) exists, that 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 security parameter index (SPI) is used to look up an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

data-call [authentication protocol | sent authentication protocol] [chap | pap]

Use the **data-call authentication protocol** and **data-call sent authentication protocol** commands to set the pre-authentication defaults for inbound demand routing calls. Use the **no** form of these commands to return to the default settings. For more detailed information on CHAP and PAP, refer to the **Technology Review** section of the command *ppp authentication <protocol>* on page 200.

Syntax Description

authentication protocol	Sets the authentication protocol expected for inbound calls.
sent authentication protocol	Sets the authentication protocol sent for inbound calls.
chap	Configures CHAP authentication.
pap	Configures PAP authentication.

Default Values

By default, there is no configuration for authentication.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

There are certain PPP parameters that must be known before PPP can negotiate an inbound call when using demand routing. To ensure PPP convergence, it is recommended (in most cases) that demand routing interfaces use the same settings as those specified in the **data-call** commands. If the PPP parameters do not match the authenticated user, the link is renegotiated.

Usage Examples

The following example sets the authentication protocol expected for incoming calls to CHAP. The router will then authenticate the peer using CHAP:

```
(config)#data-call authentication protocol chap
```

The following example sets the authentication protocol sent for incoming calls to PAP. This router may be authenticated by the peer using PAP:

```
(config)#data-call sent authentication protocol pap
```

data-call [mtu *<number>* | multilink]

Use the **data-call** commands to set the pre-authentication defaults for maximum transmit unit (MTU) size or to enable multilink for inbound demand routing calls. Use the **no** form of each command to return to the factory default settings. See the *mtu <size>* on page 198 for more detailed syntax descriptions.

Syntax Description

mtu *<number>*	Sets the maximum size for the transmit unit. Valid range: 64 to 1520.
multilink	Enables the negotiation of multilink MRU size for inbound calls.

Default Values

By default, the MTU size is 1500 and multilink is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

There are certain PPP parameters that must be known before PPP can negotiate an inbound call when using demand routing. To ensure PPP convergence, it is recommended (in most cases) that demand routing interfaces use the same settings as those specified in the **data-call** commands. The **data-call mtu** *<number>* command sets the MTU and controls the negotiated maximum receive unit (MRU) size during incoming calls for link control protocol (LCP) negotiation. If the PPP parameters do not match the authenticated user, the link is renegotiated.

Usage Examples

The following example specifies an MTU of 1200 on the demand routing interface:

```
(config)#data-call MTU 1200
```

The following example enables multilink for inbound demand routing calls:

```
(config)#data-call multilink
```

enable password [md5] *<password>*

Use the **enable password** command to define a password (with optional encryption) for accessing the Enable mode. Use the **no enable password** command to remove a configured password.

> NOTE *To prevent unauthorized users from accessing the configuration functions of your device, immediately install an Enable-level password.*

Syntax Description

md5	Optional. Specifies Message Digest 5 (MD5) as the encryption protocol to use when displaying the enable password during show commands. If the md5 keyword is not used, encryption is not used when displaying the Enable password during show commands
<password>	Specifies the Enable Security mode password using a string (up to 30 characters in length).

Default Values

By default, there is no configured enable password.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

To provide extra security, the AOS can encrypt the Enable password when displaying the current configuration. For example, the following is a **show configuration** printout (password portion) with an unencrypted Enable password (ADTRAN):

```
!
enable password ADTRAN
!
```

Alternately, the following is a **show configuration** printout (password portion) with an Enable password of ADTRAN using MD5 encryption:

```
!
enable password md5 encrypted 5aa5fbae7d01a90e79fb57705ce74676
!
```

event-history on

Use the **event-history on** command to enable event logging for the AOS system. Event log messages will not be recorded unless this command has been issued (regardless of the **event-history priority** configured). The event log may be displayed using the **show event-history** command. Use the **no** form of this command to disable the event log.

Syntax Description

No subcommands.

Default Values

By default, the AOS event logging capabilities are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The event history provides useful information regarding the status of the system and individual port states. Use the event history as a troubleshooting tool when identifying system issues. The following is a sample event history log.

```
#show event-history
Using 526 bytes
2002.07.12 15:34:01 T1.t1 1/1 Yellow
2002.07.12 15:34:01 INTERFACE_STATUS.t1 1/1 changed state to down.
2002.07.12 15:34:02 T1.t1 1/1 No Alarms
2002.07.12 15:34:02 INTERFACE_STATUS.t1 1/1 changed state to up.
2002.07.12 15:34:03 INTERFACE_STATUS.eth 0/1 changed state to up.
2002.07.12 15:34:10 OPERATING_SYSTEM Warm Start
2002.07.12 15:34:12 PPP.NEGOTIATION LCP up
2002.07.12 15:34:12 PPP.NEGOTIATION IPCP up
```

Usage Examples

The following example enables the AOS event logging feature:

```
(config)#event-history on
```

event-history priority [error | fatal | info | notice | warning]

Use the **event-history priority** command to set the threshold for events stored in the event history. All events with the specified priority or higher will be kept for viewing in the local event log. The event log may be displayed using the **show event-history** command. Use the **no** form of this command to keep specified priorities from being logged.

Syntax Description

Sets the minimum priority threshold for logging messages to the event history. The following priorities are available (ranking from lowest to highest):

error	Logs events with **error** and **fatal** priorities.
fatal	Logs only events with a **fatal** priority.
info	Logs all events.
notice	Logs events with **notice**, **warning**, **error**, and fatal priorities.
warning	Logs events with **warning**, **error**, and **fatal** priorities.

Default Values

By default, no event messages are logged to the event history.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The event history provides useful information regarding the status of the system and individual port states. Use the event history as a troubleshooting tool when identifying system issues. The following is a sample event history log.

```
Router#show event-history
Using 526 bytes
2002.07.12 15:34:01 T1.t1 1/1 Yellow
2002.07.12 15:34:01 INTERFACE_STATUS.t1 1/1 changed state to down.
2002.07.12 15:34:02 T1.t1 1/1 No Alarms
2002.07.12 15:34:02 INTERFACE_STATUS.t1 1/1 changed state to up.
2002.07.12 15:34:03 INTERFACE_STATUS.eth 0/1 changed state to up.
2002.07.12 15:34:10 OPERATING_SYSTEM Warm Start
2002.07.12 15:34:12 PPP.NEGOTIATION LCP up
2002.07.12 15:34:12 PPP.NEGOTIATION IPCP up
```

Usage Examples

The following example logs all events to the event history:

```
(config)#event-history priority info
```

exception report [filename *<filename>*]

Use the **exception report** command to specify the output filename for the exception report.

Syntax Description

filename *<filename>*	Optional. Specifies a filename for the exception report other than the default filename.

Default Values

By default, the exception report filename is **exception report-yyyyMMddHHmmss**. (The yyyyMMddHHmmss will be automatically replaced with the actual year, month, day, hour, minutes, and seconds.)

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Example

The following example specifies the output filename for an exception report:

```
(config)#exception report file-name example
(config)#exit
#exception report generate
Exception report generated.
#show flash
   1744 startup-config
  45676 example-20050708080537
#config t
(config)#no exception report file-name
(config)#exit
Appropriate commands must be issued to preserve configuration.
#exception report generate
Exception report generated.
#show flash
   1744 startup-config
  45676 example-20050708080537
  45900 exception-report-20050708080552
```

ftp authentication *<listname>*

Use the **ftp authentication** command to attach AAA login authentication lists to the FTP server (refer to *aaa authorization commands <level> [<listname> | default] [group <groupname> | group tacacs+ | if-authenticated | none]* on page 292 for more information). This list is only used if the AAA subsystem has been activated with the **aaa on** command.

Syntax Description

<listname>	Specifies the named list created with the **aaa authentication login** command. Enter **default** to use the AAA default login list.

Default Values

There is no default configuration for the list. If AAA is turned on but no **ftp authentication** list has been assigned, FTP denies all login attempts.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example attaches the authentication list, **MyList**, to the FTP server:

```
(config)#ftp authentication MyList
```

The following example specifies that the AOS use the default AAA login list for FTP authentication:

```
(config)#ftp authentication default
```

hostname *<name>*

Creates a name used to identify the unit. This alphanumeric string should be used as a unique description for the unit. This string will be displayed in all prompts.

Syntax Description

<name>	Identifies the unit using an alphanumeric string up to 32 characters.

Default Values

<name>	Router

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example creates a hostname for the AOS device of **ATL_RTR** to identify the system as the Atlanta router:

```
(config)#hostname ATL_RTR
```

interface *<interface>* [*<slot/port>* | *<interface id>*] [point-to-point]

Use the **interface** command to activate the interface command set for the specified physical or virtual interface. Use the **no** form of this command to delete a configured interface. To activate the interface, enter the **no shutdown** command from within the specific interface command set. For example, (config-ppp 7)#**no shutdown**.

Syntax Description

<interface>	Identifies the physical port type of the installed Network Interface Module (NIM), Dial-Backup Interface Module (DIM), or Ethernet port. Type **interface ?** for a complete list of valid interfaces.
<slot/port>	Specifies an interface based on its physical location (slot and port). For example, if you have a T1/DSX-1 NIM installed in Slot 1 of an AOS product: • The **WAN-T1** port would be specified in the CLI as **t1 1/1**. • The **DSX-1** port would be specified as **t1 1/2**. • If (for example) a **BRI DIM** backup module is also installed, then the **DBU** port of the NIM card would be specified as **bri 1/3**. • If you are specifying a port that is built into the base unit (e.g., the Ethernet port), the slot number is **0**. For example, the Ethernet (**LAN**) port would be specified as **eth 0/1**.
<interface id>	Specifies the numerical interface ID using a numerical string. Valid range is 1 to 1024. To specify a sub-interface the following syntax applies: **interface atm** *<interface id>***.***<sub-interface id>*. Valid range is 1 to 255.
point-to-point	Optional. Identifies the interface as a point-to-point link (versus multilink). Valid only on interfaces that support point-to-point (e.g., ATM and Frame Relay). By default, all created ATM and Frame Relay interfaces are point-to-point.

Default Values

No default values required for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command expanded to include loopback interface.
Release 8.1	Command expanded to include ATM interface.
Release 9.1	Command expanded to include HDLC interface.
Release 11.1	Command expanded to include demand, FXO, and PRI interfaces.

Usage Examples

The following example enters the serial interface mode for a serial module installed in slot 1:

```
(config)#interface serial 1/1
(config-ser 1/1)#
```

ip access-list extended *<listname>*

Use the **ip access-list extended** command to create an empty access list and enter the extended access-list. Use the **no** form of this command to delete an access list and all the entries contained in it.

The following lists the complete syntax for the **ip access-list extended** commands:

<action> <protocol> <source ip> <source port> <destination ip> <destination port>

Example:

Source IP Address

[**permit** | **deny**] [**ip | tcp | udp**] [**any | host** *<A.B.C.D>* **|** *<A.B.C.D> <W.W.W.W>*]

*<source port>** [**any | host** *<A.B.C.D>* **|** *<A.B.C.D> <W.W.W.W>*] *<destination port>**

Destination IP Address

Example:

Source IP Address

[**permit** | **deny**] **icmp** [**any | host** *<A.B.C.D>* **|** *<A.B.C.D> <W.W.W.W>*]

[**any | host** *<A.B.C.D>* **|** *<A.B.C.D> <W.W.W.W>*] *<icmp-type>* <icmp-code>* <icmp-message>**

Destination IP Address

* = optional

Syntax Description

<listname>	Identifying the configured access list using an alphanumeric descriptor. All access list descriptors are case-sensitive.
<protocol>	Specifies the data protocol such as IP, ICMP, TCP, UDP, or a specific protocol (range: 0 to 255).
<source ip>	Specifies the source IP address used for packet matching. IP addresses can be expressed in one of three ways: 1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword. 2. Using the **host** *<A.B.C.D>* to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253. 3. Using the *<A.B.C.D> <wildcard>* format to match all IP addresses in a "range." Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a "don't care". For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.
<source port>	Optional. The source port is used only when *<protocol>* is **tcp** or **udp**.

The following keywords and port numbers are supported for the <*source port*> field:

any	Matches any destination port.
eq <*port number*>	Matches only packets on a given port number.
gt <*port number*>	Matches only packets with a port number higher than the one listed.
host <*port number*>	Matches a single destination host.
lt <*port number*>	Matches only packets with a port number lower than the one listed.
neq <*port number*>	Matches only packets that do not contain the specified port number.
range <*port number*>	Matches only packets that contain a port number specified in the listed range.

The <*port number*> may be specified using the following syntax: <0-65535>. Specifies the port number used by TCP or UDP to pass information to upper layers. All ports below 1024 are considered well-known ports and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications

<*port list*> The AOS provides a condensed list of port numbers that may be entered using a text name.

The following is the list of UDP port numbers that may be identified using the text name (in **bold**):

biff (Port 512)
bootpc (Port 68)
bootps(Port 67)
discard (Port 9)
dnsix (Port 195)
domain (Port 53)
echo (Port 7)
isakmp (Port 500)
mobile-ip (Port 434)
nameserver (Port 42)
netbios-dgm (Port 138)
netbios-ns (Port 137)
netbios-ss (Port 139)
ntp (Port 123)
pim-auto-rp (Port 496)
rip (Port 520)
snmp (Port 161)
snmptrap (Port 162)
sunrpc (Port 111)
syslog (Port 514)
tacacs (Port 49)
talk (Port 517)
tftp (Port 69)
time (Port 37)
who (Port 513)
xdmcp (Port 177)

The following is the list of TCP port numbers that may be identified using the text name (in **bold**):

bgp (Port 179)
chargen (Port 19)
cmd (Port 514)
daytime (Port 13)
discard (Port 9)
domain (Port 53)
echo (Port 7)
exec (Port 512)
finger (Port 79)
ftp (Port 21)
gopher (Port 70)
hostname (Port 101)
ident (Port 113)
irc (Port 194)
klogin (Port 543)
kshell (Port 544)
login (Port 513)
lpd (Port 515)
nntp (Port 119)
pim-auto-rp (Port 496)
pop2 (Port 109)
pop3 (Port 110)
smtp (Port 25)
sunrpc (Port 111)
syslog (Port 514)
tacacs (Port 49)
talk (Port 517)
tftp (Port 69)
telnet (Port 23)
time (Port 37)
uucp (Port 540)
whois (Port 43)
www (Port 80)

<destination ip> Specifies the destination IP address used for packet matching.

IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <A.B.C.D> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the *<A.B.C.D> <wildcard>* format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

<destination port> Optional. Specifies the destination port. Only valid when *<protocol>* is **tcp** or **udp** (Refer to previously listed *<source port>* for more details).

<icmp-type> Optional. Filters packets using ICMP defined (and numbered) messages carried in IP datagrams (used to send error and control information). Valid range is 0 to 255.

<icmp-code> Optional. Filters ICMP packets that are filtered using the ICMP message type (using the *<icmp-type>* keyword) may also be filtered using the ICMP message code (valid range: 0 to 255).

An *<icmp-type>* must be specified when entering an *<icmp-code>.*

<icmp-message> Optional. Filters packets using ICMP descriptive message rather than the corresponding type and code associations.

Default Values

By default, all AOS security features are disabled and there are no configured access lists.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1 Command was introduced.

Functional Notes

Access control lists (ACLs) are used as packet selectors by other AOS systems; by themselves they do nothing. ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An ACL entry contains two parts: an action (permit or deny) and a packet pattern. A permit ACL is used to allow packets (meeting the specified pattern) to enter the router system. A deny ACL advances the AOS to the next access policy entry. The AOS provides two types of ACLs: standard and extended. Standard ACLs allow source IP address packet patterns only. Extended ACLs may specify patterns using most fields in the IP header and the TCP or UDP header.

ACLs are performed in order from the top of the list down. Generally, the most specific entries should be at the top and the most general at the bottom.

The following commands are contained in the access-list extended mode:

remark Associates a descriptive tag (up to 80 alphanumeric characters enclosed in quotation marks) to the access list. Enter a functional description for the list such as “This list blocks all outbound web traffic”.

log Logs a message (if debug access-list is enabled for this access list) when the access list finds a packet match.

Usage Examples

The following example creates an access list **AllowIKE** to allow all IKE (UDP Port 500) packets from the 190.72.22.55.0/24 network:

```
(config)#ip access-list extended AllowIKE
(config-ext-nacl)#permit udp 190.72.22.55.0 0.0.0.255 eq 500 any eq 500
```

For more details, refer to the *ADTRAN OS System Documentation* CD or the ADTRAN website (www.adtran.com) for technical support notes regarding access-list configuration.

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:

Enable the security features of the AOS using the **ip firewall** command.

Step 2:

Create an access control list (using the **ip access-list** command) to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:

Create an access control policy (using the **ip policy-class** command) that uses a configured access list. AOS access policies are used to allow, discard, or manipulate (using **NAT)** data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>

All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>

All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload [policy]**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network. The **policy** option specifies the destination policy class.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

CAUTION *Before applying an access control policy to an interface, verify your Telnet connection will not be affected by the policy. If a policy is applied to the interface you are connecting through and it does not allow Telnet traffic, your connection will be lost.*

Step 4:

Apply the created access control policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the Ethernet 0/1 interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#access-policy MatchAll
```

ip access-list standard *<listname>* [permit | deny] *<ip address>*

Use the **ip access-list standard** command to create an empty access list and enter the standard access-list. Use the **no** form of this command to delete an access list and all the entries contained in it.

The following lists the complete syntax for the **ip access-list standard** commands:

ip access-list standard *<listname>* **[permit | deny] any [permit | deny] host** *<ip address>*
[permit | deny] *<ip address> <wildcard>*

Syntax Description

<listname> Identifies the configured access list using an alphanumeric descriptor. All access list descriptors are case-sensitive.

[permit | deny] Permits or denies entry to the routing system for specified packets.

<ip address> Specifies the source IP address used for packet matching.

IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** *<A.B.C.D>* to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the *<A.B.C.D> <wildcard>* format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Default Values

By default, all AOS security features are disabled and there are no configured access lists.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 9000 Series units.

Command History

Release 2.1 Command was introduced.

Functional Notes

Access control lists are used as packet selectors by access policies (ACPs); by themselves they do nothing. ACLs are composed of an ordered list of entries with an implicit **deny all** at the end of each list. An ACL entry contains two parts: an action (permit or deny) and a packet pattern. A permit ACL is used to allow packets (meeting the specified pattern) to enter the router system. A deny ACL advances the AOS to the next access policy entry. The AOS provides two types of ACLs: standard and extended. Standard ACLs allow source IP address packet patterns only. Extended ACLs may specify patterns using most fields in the IP header and the TCP or UDP header.

ACLs are performed in order from the top of the list down. Generally the most specific entries should be at the top and the most general at the bottom.

The following commands are contained in the **access-list standard**:

remark

Associates a descriptive tag (up to 80 alphanumeric characters enclosed in quotation marks) to the access list. Enter a functional description for the list such as “This list blocks all outbound web traffic.”

log

Logs a message (if **debug access-list** is enabled for this access list) when the access list finds a packet match.

permit or deny any

Uses the **any** keyword to match any IP address received by the access list. For example, the following allows all packets through the configured access list:

```
(config)#ip access-list standard MatchAll
(config-std-nacl)#permit any
```

permit or deny host *<ip address>*

Uses the **host** *<A.B.C.D>* keyword to specify a single host address. For example, the following allows all traffic from the host with an IP address of 196.173.22.253.

```
(config)#ip access-list standard MatchHost
(config-std-nacl)#permit host 196.173.22.253
```

permit or deny *<ip address> <wildcard>*

Uses the *<A.B.C.D> <wildcard>* format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, the following denies all traffic from the 192.168.0.0/24 network:

```
(config)#ip access-list standard MatchNetwork
(config-std-nacl)#deny 192.168.0.0 0.0.0.255
```

Usage Examples

The following example creates an access list **UnTrusted** to deny all packets from the 190.72.22.248/30 network:

```
(config)#ip access-list standard UnTrusted
(config-std-nacl)#deny 190.72.22.248 0.0.0.3
```

For more details, refer to the *ADTRAN OS System Documentation* CD or the ADTRAN website (www.adtran.com) for technical support notes regarding access list configuration.

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of the AOS using the **ip firewall** command.

Step 2:
Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:
Create an access policy that uses a configured access list. AOS access policies are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each ACP consists of a selector (access list) and an action (allow, discard, NAT). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>
All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>
All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>
All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload [policy]**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network. The **policy** option specifies the destination policy class.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

CAUTION

Before applying an access control policy to an interface, verify your Telnet connection will not be affected by the policy. If a policy is applied to the interface you are connecting through and it does not allow Telnet traffic, your connection will be lost.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the Ethernet 0/1 interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#access-policy MatchAll
```

ip classless

Use the **ip classless** command to forward classless packets to the best supernet route available. A classless packet is a packet addressed for delivery to a subnet of a network with no default network route.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the Netvanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

AOS products only function in classless mode. You cannot disable this feature.

Usage Examples

The following example enables the system to forward classless packets:

```
(config)#ip classless
```

ip crypto

Use the **ip crypto** command to enable AOS VPN functionality and allow crypto maps to be added to interfaces. Use the **no** form of this command to disable the VPN functionality.

> NOTE *Disabling the AOS security features (using the **no ip crypto** command) does not affect VPN configuration settings (with the exception of the removal of all crypto maps from the interfaces). All other configuration parameters will remain intact, and VPN functionality will be disabled.*

> NOTE *For VPN configuration example scripts, refer to the **VPN Configuration Guide** located on the **ADTRAN OS Documentation** CD provided with your unit.*

Syntax Description

No subcommands.

Default Values

By default, all AOS VPN functionality is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

VPN-related settings will not go into effect until you enable VPN functionality using the **ip crypto** command. The AOS allows you to perform all VPN-related configuration prior to enabling **ip crypto**, with the exception of assigning a **crypto map** to an interface. The **no ip crypto** command removes all crypto maps from the interfaces. Enabling **ip crypto** enables the IKE server on UDP Port 500. The **no** form of this command disables the IKE server on UDP Port 500.

Usage Examples

The following example enables VPN functionality:

```
(config)#ip crypto
```

ip default-gateway *<ip address>*

Use the **ip default-gateway** command to specify a default gateway if (and only if) IP routing is NOT enabled on the unit. Use the **ip route** command to add a default route to the route table when using IP routing functionality.

Syntax Description

<ip address>	Specifies the default gateway IP address in the form of dotted decimal notation (example: 192.22.71.50).

Default Values

By default, there is no configured default-gateway.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Only use the **ip default-gateway** when IP routing is disabled on the router. For all other cases, use the **ip route 0.0.0.0 0.0.0.0** *<ip address>* command.

Usage Examples

The following example disables IP routing and configures a default gateway for 192.22.71.50:

```
(config)#no ip routing
(config)#ip default-gateway 192.22.71.50
```

ip dhcp-server database local

Use the **ip dhcp-server database local** command to configure a DHCP database agent with local bindings. Use the **no** form of this command to disable this option.

Syntax Description

No subcommands.

Default Values

No default values.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example configures the DHCP database agent with local bindings:

```
(config)#ip dhcp-server database local
```

ip dhcp-server excluded-address *<start ip> <end ip>*

Use the **ip dhcp-server excluded-address** command to specify IP addresses that cannot be assigned to DHCP clients. Use the **no** form of this command to remove a configured IP address restriction.

Syntax Description

<start ip>	Specifies the lowest IP address (using dotted decimal notation) in the range OR a single IP address to be excluded.
<end ip>	Optional. Specifies the highest IP address (using dotted decimal notation) in the range. This field is not required when specifying a single IP address.

Default Values

By default, there are no excluded IP addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

The AOS DHCP server (by default) allows all IP addresses for the DHCP pool to be assigned to requesting clients. This command is used to ensure that the specified address is never assigned by the DHCP server. When static addressed hosts are present in the network, it is helpful to exclude the IP addresses of the host from the DHCP IP address pool. This will avoid IP address overlap.

Usage Examples

The following example excludes an IP address of 172.22.5.100 and the range 172.22.5.200 through 172.22.5.250:

```
(config)#ip dhcp-server excluded-address 172.22.5.100
(config)#ip dhcp-server excluded-address 172.22.5.200 172.22.5.250
```

ip dhcp-server ping packets *<#packets>*

Use the **ip dhcp-server ping packets** command to specify the number of ping packets the DHCP server will transmit before assigning an IP address to a requesting DHCP client. Transmitting ping packets verifies that no other hosts on the network are currently configured with the specified IP address. Use the **no** form of this command to prevent the DHCP server from using ping packets as part of the IP address assignment process.

Syntax Description

<#packets>	Specifies the number of DHCP ping packets sent on the network before assigning the IP address to a requesting DHCP client

Default Values

By default, the number of DHCP server ping packets is set at 2 packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Before assigning an IP address to a requesting client, the AOS DHCP server transmits a ping packet on the network to verify there are no other network hosts already configured with the specified address. If the DHCP server receives no reply, the IP address is assigned to the requesting client and added to the DHCP database as an assigned address. Configuring the **ip dhcp-server ping packets** command with a value of **0** prevents the DHCP server from using ping packets as part of the IP address assignment process.

Usage Examples

The following example configures the DHCP server to transmit four ping packets before assigning an address:

```
(config)#ip dhcp-server ping packets 4
```

ip dhcp-server ping timeout *<milliseconds>*

Use the **ip dhcp-server ping timeout** command to specify the interval (in milliseconds) the DHCP server will wait for a response to a transmitted DHCP ping packet. The DHCP server transmits ping packets before assigning an IP address to a requesting DHCP client. Transmitting ping packets verifies that no other hosts on the network are currently configured with the specified IP address. Use the **no** form of this command to return to the default timeout interval.

Syntax Description

<milliseconds>	Specifies the number of milliseconds (valid range: 1 to 1000) the DHCP server will wait for a response to a transmitted DHCP ping packet.

Default Values

By default, the **ip dhcp-server ping timeout** is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Before assigning an IP address to a requesting client, the AOS DHCP server transmits a ping packet on the network to verify there are no other network hosts already configured with the specified address. If the DHCP server receives no reply, the IP address is assigned to the requesting client and added to the DHCP database as an assigned address.

Usage Examples

The following example configures the DHCP server to wait 900 milliseconds for a response to a transmitted DHCP ping packet before considering the ping a failure:

```
(config)#ip dhcp-server ping timeout 900
```

ip dhcp-server pool *<name>*

Use the **ip dhcp-server pool** command to create a DHCP address pool and enter the DHCP pool. Use the **no** form of this command to remove a configured DHCP address pool. Refer to the section *DHCP Pool Command Set* on page 1145 for more information.

Syntax Description

<name>	Identifies the configured DHCP server address pool using an alphanumeric string (up to 32 characters in length).

Default Values

By default, there are no configured DHCP address pools.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Use the **ip dhcp-server pool** to create multiple DHCP server address pools for various segments of the network. Multiple address pools can be created to service different segments of the network with tailored configurations.

Usage Examples

The following example creates a DHCP server address pool (labeled **SALES**) and enters the DHCP server pool mode:

```
(config)#ip dhcp-server pool SALES
(config-dhcp)#
```

ip domain-lookup

Use the **ip domain-lookup** command to enable the IP domain naming system (DNS), allowing DNS-based host translation (name-to-address). Use the **no** form of this command to disable DNS.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

Use the **ip domain-lookup** command to enable the DNS client in the router. This will allow the user to input web addresses instead of IP addresses for applications such as ping, Telnet, and traceroute.

Usage Examples

The following example enables DNS:

```
(config)#ip domain-lookup
```

ip domain-name *<name>*

Use the **ip domain-name** command to define a default IP domain name to be used by the AOS to resolve host names. Use the **no** form of this command to disable this function.

Syntax Description

<name>	Specifies the default IP domain name used to resolve unqualified host names. Do not include the initial period that separates the unresolved name from the default domain name.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

Use the **ip domain-name** command to set a default name which will be used to complete any IP host name that is invalid (i.e., any name that is not recognized by the name server). When this command is enabled, any IP host name that is not initially recognized will have the **ip domain-name** appended to it and the request will be resent.

Usage Examples

The following example defines **adtran** as the default domain name:

```
(config)#ip domain-name adtran
```

ip domain-proxy

Use the **ip domain-proxy** command to enable DNS proxy for the router. This enables the router to act as a proxy for other units on the network.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

When this command is enabled, incoming DNS requests will be handled by the router. It will first search its host table for the query, and if it is not found there the request will be forwarded to the servers configured with the **ip name-server** command.

Usage Examples

The following example enables DNS proxy:

```
(config)#ip domain-proxy
```

ip firewall

Use the **ip firewall** command to enable AOS security features including access control policies and lists, Network Address Translation (NAT), and the stateful inspection firewall. Use the **no** form of this command to disable the security functionality.

> NOTE
>
> *Disabling the AOS security features (using the **no ip firewall** command) does not affect security configuration. All configuration parameters will remain intact, but no security data processing will be attempted.*

> NOTE
>
> *For information regarding the use of OSPF with **ip firewall** enabled, refer to the **Functional Note** for router ospf* on page 441.
>
> *Regarding the use of IKE negotiation for VPN with **ip firewall** enabled, there can be up to six channel groups with 2 to 8 interfaces per group. Dynamic protocols are not yet supported (only static). A physical interface can be a member of only one channel group.*

Syntax Description

No subcommands.

Default Values

By default, all AOS security features are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

This command enables firewall processing for all interfaces with a configured policy class. Firewall processing consists of the following functions:

Attack Protection: Detects and discards traffic that matches profiles of known networking exploits or attacks.

Session Initiation Control: Allows only sessions that match traffic patterns permitted by access-control policies to be initiated through the router.

Ongoing Session Monitoring and Processing: Each session that has been allowed through the router is monitored for any irregularities that match patterns of known attacks or exploits. This traffic will be dropped. Also, if NAT is configured, the firewall modifies all traffic associated with the session according to the translation rules defined in NAT access policies. Finally, if sessions are inactive for a user-specified amount of time, the session will be closed by the firewall.

Application Specific Processing: Certain applications need special handling to work correctly in the presence of a firewall. AOS uses application-level gateways (ALGs) for these applications.

The AOS includes several security features to provide controlled access to your network. The following features are available when security is enabled (using the **ip firewall** command):

1. Stateful Inspection Firewall

The AOS (and your unit) act as an ALG and employ a stateful inspection firewall that protects an organization's network from common cyber attacks including TCP syn-flooding, IP spoofing, ICMP redirect, land attacks, ping-of-death, and IP reassembly problems. In addition, further security is added with use of Network Address Translation (NAT) and Port Address Translation (PAT) capability.

2. Access Policies

AOS access control policies (ACPs) are used to allow, discard, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded.

3. Access Lists

Access control lists (ACLs) are used as packet selectors by ACPs; by themselves they do nothing. ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A permit ACL is used to permit packets (meeting the specified pattern) to enter the router system. A deny ACL advances the AOS to the next access policy entry. The AOS provides two types of ACLs: **standard** and **extended**. Standard ACLs allow source IP address packet patterns only. Extended ACLs may specify patterns using most fields in the IP header and the TCP or UDP header.

Usage Examples

The following example enables the AOS security features:

```
(config)#ip firewall
```

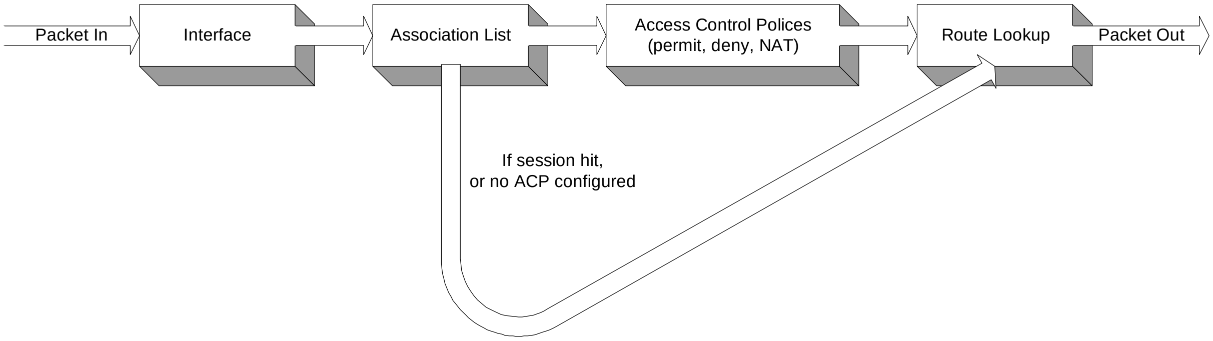
Technology Review

Concepts:

Access control using the AOS firewall has two fundamental parts: Access Control Lists (ACLs) and Access Policy Classes (ACPs). ACLs are used as packet selectors by other AOS systems; by themselves they do nothing. ACPs consist of a selector (ACL) and an action (allow, discard, NAT). ACPs integrate both allow and discard policies with NAT. ACPs have no effect until they are assigned to a network interface.

Both ACLs and ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry in the list and progresses through the entries until it finds a match. The first entry that matches is executed.

Packet Flow:



Case 1: Packets from interfaces with a configured policy class to any other interface

ACPs are applied when packets are received on an interface. If an interface has not been assigned a policy class, by default it will allow all received traffic to pass through. If an interface has been assigned a policy class but the firewall has not been enabled with the **ip firewall** command, traffic will flow normally from this interface with no firewall processing.

Case 2: Packets that travel in and out a single interface with a configured policy class

These packets are processed through the ACPs as if they are destined for another interface (identical to Case 1).

Case 3: Packets from interfaces without a configured policy class to interfaces with one

These packets are routed normally and are not processed by the firewall. The **ip firewall** command has no effect on this traffic.

Case 4: Packets from interfaces without a configured policy class to other interfaces without a configured policy class

This traffic is routed normally. The **ip firewall** command has no effect on this traffic.

Attack Protection:

When the **ip firewall** command is enabled, firewall attack protection is enabled. The AOS blocks traffic (matching patterns of known networking exploits) from traveling through the device. For some of these attacks, the user may manually disable checking/blocking while other attack checks are always on anytime the firewall is enabled.

The table (on the following pages) outlines the types of traffic discarded by the firewall attack protection engine. Many attacks use similar invalid traffic patterns; therefore attacks other than the examples listed below may also be blocked by the firewall. To determine if a specific attack is blocked by the AOS firewall, please contact ADTRAN technical support.

Invalid Traffic Pattern	Manually Enabled?	AOS Firewall Response	Common Attacks
Larger than allowed packets	No	Any packets that are longer than those defined by standards will be dropped.	Ping of Death
Fragmented IP packets that produce errors when attempting to reassemble	No	The firewall intercepts all fragments for an IP packet and attempts to reassemble them before forwarding to destination. If any problems or errors are found during reassembly, the fragments are dropped.	SynDrop, TearDrop, OpenTear, Nestea, Targa, Newtear, Bonk, Boink
Smurf Attack	No	The firewall will drop any ping responses that are not part of an active session.	Smurf Attack
IP Spoofing	No	The firewall will drop any packets with a source IP address that appears to be spoofed. The IP route table is used to determine if a path to the source address is known (out of the interface from which the packet was received). For example, if a packet with a source IP address of 10.10.10.1 is received on interface fr 1.16 and no route to 10.10.10.1 (through interface fr 1.16) exists in the route table, the packet is dropped.	IP Spoofing
ICMP Control Message Floods and Attacks	No	The following types of ICMP packets are allowed through the firewall: echo, echo-reply, TTL expired, dest. Unreachable, and quench. These ICMP messages are only allowed if they appear to be in response to a valid session. All others are discarded.	Twinge

Invalid Traffic Pattern	Manually Enabled?	AOS Firewall Response	Common Attacks
Attacks that send TCP URG packets	Yes	Any TCP packets that have the URG flag set are discarded by the firewall.	Winnuke, TCP XMAS Scan
Falsified IP Header Attacks	No	The firewall verifies that the packet's actual length matches the length indicated in the IP header. If it does not, the packet is dropped.	Jolt/Jolt2
Echo	No	All UDP echo packets are discarded by the firewall.	Char Gen
Land Attack	No	Any packets with the same source and destination IP addresses are discarded.	Land Attack
Broadcast Source IP	No	Packets with a broadcast source IP address are discarded.	
Invalid TCP Initiation Requests	No	TCP SYN packets that have ack, urg rst, or fin flags set are discarded.	
Invalid TCP Segment Number	No	The sequence numbers for every active TCP session are maintained in the firewall session database. If the firewall received a segment with an unexpected (or invalid) sequence number, the packet is dropped.	
IP Source Route Option	No	All IP packets containing the IP source route option are dropped.	

Application Specific Processing:

The following applications and protocols require special processing to operate concurrently with NAT/firewall functionality. The AOS firewall includes ALGs for handling these applications and protocols:

AOL Instant Messenger (AIM®)
VPN ALGS: ESP and IKE
FTP
H.323: H.245 Q.931 ASN1 PER decoding and Encoding
ICQ®
IRC
Microsoft® Games
Net2Phone
PPTP
Quake®
Real-Time Streaming Protocol
SMTP
HTTP
CUseeme
SIP
L2TP
PcAnywhere™
SQL
Microsoft Gaming Zone

To determine if a specific application requires special processing, contact technical support. ADTRAN at *www.adtran.com.*

ip firewall alg [ftp | h323 | pptp]

Use the **ip firewall alg** command to enable the application-level gateway (ALG) for a particular application. Use the **no** form of this command to disable ALG for the application.

Syntax Description

ftp	Enables the FTP ALG.
h323	Enables the H323 ALG.
pptp	Enables the PPTP ALG.

Default Values

By default, the ALG for FTP, H323, and PPTP are enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 10.1	H323 was added.

Functional Notes

Enabling the Application Layer Gateway (ALG) for a specific protocol gives the firewall additional information about that complex protocol and causes the firewall to perform additional processing for packets of that protocol. When the ALG is disabled, the firewall treats the complex protocol as any other simple protocol. The firewall needs no special knowledge to work well with simple protocols.

WARNING

Disabling the IP firewall ALG may cause the firewall to block some of the traffic for the specified protocol.

Usage Examples

The following example disables ALG for FTP:

```
(config)#no ip firewall alg ftp
```

ip firewall alg sip udp *<port#>*

Use the **ip firewall alg sip udp** command to configure the user datagram protocol (UDP) port for Session Initiation Protocol (SIP) application-level gateways (ALG). Use the **no** form of this command to return to the default settings.

Syntax Description

udp *<port#>*	Sets the UDP port. Valid range: 1 to 65,535.

Default Values

By default, the ALG for SIP is enabled and the UDP port is set to 5060.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables port 1020 for UDP:

```
(config)#ip firewall alg sip udp 1020
```

ip firewall attack-log threshold *<value>*

Use the **ip firewall attack-log threshold** command to specify the number of attack mounting attempts the AOS will identify before generating a log message. Use the **no** form of this command to return to the default threshold.

> NOTE *The AOS security features must be enabled (using the* ***ip firewall*** *command) for the stateful inspection firewall to be activated.*

Syntax Description

<*value*>	Specifies the number of attack mounting attempts the AOS will identify before generating a log message (valid range: 0 to 4,294,967,295).

Default Values

By default, the **ip firewall attack-log threshold** is set at 100.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a threshold of 25 attacks before generating a log message:

```
(config)#ip firewall attack-log threshold 25
```

ip firewall check reflexive-traffic

Use the **ip firewall check reflexive-traffic** command to enable the AOS stateful inspection firewall to process traffic from a primary subnet to a secondary subnet on the same interface through the firewall. Use the **no** form of this command to disable this feature.

> NOTE *The AOS security features must be enabled (using the **ip firewall** command) for the stateful inspection firewall to be activated.*

Syntax Description

No subcommands.

Default Values

All AOS security features are disabled by default until the **ip firewall** command is issued at the Global Configuration prompt. In addition, the reflexive traffic check is disabled until the **ip firewall check reflexive-traffic** command is issued.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command allows the firewall to process traffic from a primary subnet to a secondary subnet on the same interface through the firewall. If enabled, this traffic will be processed through the access policy on that interface and any actions specified will be executed on the traffic.

Usage Examples

The following example enables the AOS reflexive traffic check:

```
(config)#ip firewall check reflexive-traffic
```

ip firewall check syn-flood

Use the **ip firewall check syn-flood** command to enable the AOS stateful inspection firewall to filter out phony TCP service requests and allow only legitimate requests to pass through. Use the **no** form of this command to disable this feature.

> NOTE *The AOS security features must be enabled (using the* ***ip firewall*** *command) for the stateful inspection firewall to be activated.*

Syntax Description

No subcommands.

Default Values

All AOS security features are disabled by default until the **ip firewall** command is issued at the Global Configuration prompt. In addition, the SYN-flood check is disabled until the **ip firewall check syn-flood** command is issued.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

SYN flooding is a well-known denial of service attack on TCP-based services. TCP requires a three-way handshake before actual communications begin between two hosts. A server must allocate resources to process new connection requests that are received. A potential intruder is capable of transmitting large amounts of service requests (in a very short period of time), causing servers to allocate all resources to process the phony incoming requests. Using the **ip firewall check syn-flood** command configures the AOS stateful inspection firewall to filter out phony service requests and allow only legitimate requests to pass through.

Usage Examples

The following example enables the AOS SYN-flood check:

```
(config)#ip firewall check syn-flood
```

ip firewall check winnuke

Use the **ip firewall check winnuke** command to enable the AOS stateful inspection firewall to discard all out of band (OOB) data (to protect against WinNuke attacks). Use the **no** form of this command to disable this feature.

> NOTE *The AOS security features must be enabled (using the* ***ip firewall*** *command) for the stateful inspection firewall to be activated.*

Syntax Description

No subcommands.

Default Values

All AOS security features are disabled by default until the **ip firewall** command is issued at the Global Configuration prompt. Issuing the **ip firewall** command enables the WinNuke check.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

WinNuke attack is a well-known denial of service attack on hosts running Microsoft Windows® operating systems. An intruder sends out of band (OOB) data over an established connection to a Windows user. Windows cannot properly handle the OOB data and the host reacts unpredictably. Normal shut-down of the hosts will generally return all functionality. Using the **ip firewall check winnuke** command configures the AOS stateful inspection firewall to filter all OOB data to prevent network problems.

Usage Examples

The following example enables the firewall to filter all OOB data:

```
(config)#ip firewall check winnuke
```

ip firewall policy-log threshold *<value>*

Use the **ip firewall policy-log threshold** command to specify the number of connections required by an access control policy before the AOS will generate a log message. Use the **no** form of this command to return to the default threshold.

> *The AOS security features must be enabled (using the* ***ip firewall*** *command) for the stateful inspection firewall to be activated.*

Syntax DescriptionSyntax Description

<value>	Specifies the number of access policy connections the AOS will identify before generating a log message (valid range: 0 to 4,294,967,295).

Default Values

By default, the **ip firewall policy-log threshold** is set to 100.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a threshold of 15 connections before generating a log message:

```
(config)#ip firewall policy-log threshold 15
```

ip forward-protocol udp *<port number>*

Use the **ip forward-protocol udp** command to specify the protocols and ports the AOS allows when forwarding broadcast packets. Use the **no** form of this command to disable a specified protocol or port from being forwarded.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure the AOS to forward UDP broadcast packets. Refer to ip helper-address <address>* on page 551 *for more information.*

Syntax Description

<port number> Specifies the UDP traffic type (using source port)

The following is the list of UDP port numbers that may be identified using the text name:

biff (Port 512)
bootps(Port 67)
discard (Port 9)
dnsix (Port 195)
domain (Port 53)
echo (Port 7)
isakmp (Port 500)
mobileip (Port 434)
nameserver (Port 42)
netbios-dgm (Port 138)
netbios-ns (Port 137)
netbios-ss (Port 139)
ntp (Port 123)
pim-auto-rp (Port 496)
rip (Port 520)
snmp (Port 161)
snmptrap (Port 162)
sunrpc (Port 111)
syslog (Port 514)
tacacs (Port 49)
talk (Port 517)
tftp (Port 69)
time (Port 37)
who (Port 513)
xdmcp (Port 177)

Alternately, the *<port number>* may be specified using the following syntax: <0-65535>. Specifies the port number used by UDP to pass information to upper layers. All ports below 1024 are considered well-known ports and are controlled by the Internet Assigned Numbers Authority (IANA). All ports above 1024 are dynamically assigned ports that include registered ports for vendor-specific applications.

Default Values

By default, the AOS forwards broadcast packets for all protocols and ports.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Use this command to configure the AOS to forward UDP packets across the WAN link to allow remote devices to connect to a UDP service on the other side of the WAN link.

Usage Examples

The following example forwards all Domain Name Server (DNS) broadcast traffic to the DNS server with IP address 192.33.5.99:

```
(config)#ip forward-protocol udp domain
(config)#interface eth 0/1
(config-eth 0/1)#ip helper-address 192.33.5.99
```

ip ftp access-class *<policyname>* in

Use the **ip ftp access-class in** command to assign an access policy to all self-bound File Transfer Protocol (FTP) sessions.

Syntax Description

<policyname>	Specifies the configured access policy (ACP) to apply to inbound FTP traffic.

Default Values

By default, all FTP access is allowed.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example applies the configured ACP (labeled **Inbound_FTP**) to inbound FTP traffic:

```
(config)#ip ftp access-class Inbound_FTP in
```

ip ftp agent

Use the **ip ftp agent** command to enable the file transfer protocol (FTP) agent.

Syntax Description

No subcommands.

Default Values

By default, the FTP agent is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example enables the IP FTP agent:

```
(config)#ip ftp agent
```

ip ftp source-interface *<interface>*

Use the **ip ftp source-interface** command to use the specified interface's IP address as the source IP address for FTP traffic transmitted by the unit. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<interface>	Specifies the interface to be used as the source IP address for FTP traffic. Type **ip ftp source-interface?** for a complete list of valid interfaces.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.
Release 9.1	Command expanded to include HDLC interface.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for FTP traffic:

```
(config)#ip ftp source-interface loopback 1
```

ip host *<name> <address1>*

Use the **ip host** command to define an IP host name. This allows you to statically map host names and addresses in the host cache. Use the **no** form of this command to remove defined maps.

Syntax Description

<name>	Defines the name of the host.
<address1>	Specifies IP address associated with this IP host.

Default Values

By default, the host table is empty.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The name may be any combination of numbers and letters as long as it is not a valid IP address or does not exceed 256 characters.

Usage Examples

The following example defines two static mappings:

```
(config)#ip host mac 10.2.0.2
(config)#ip host dal 172.38.7.12
```

ip igmp join *<group-address>*

Use the **ip igmp join** command to instruct the router stack to join a specific group. The stack may join multiple groups.

Syntax Description

<group-address>	Specifies the IP address of a multicast group.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command aids in debugging, allowing the router's IP stack to connect to and respond on a multicast group. The local stack operates as an IGMP host on the attached segment. In multicast stub applications, the global helper address takes care of forwarding IGMP joins/responses on the upstream interface. The router may respond to ICMP echo requests for the joined groups.

Usage Examples

The following example configures the unit to join with the specified multicast group:

```
(config)#ip igmp join 172.0.1.50
```

ip load-sharing [per-destination | per-packet]

Use the **ip load-sharing** command to configure whether parallel routes in the route table are used to load-share forwarded packets. If this command is disabled, the route table uses a single “best” route for a given subnet. If this command is enabled, the route table can use multiple “best” routes and alternate between them.

Syntax Description

per-destination	Specifies that the route used for forwarding a packet be based on a hash of the source and destination IP address in the packet.
per-packet	Specifies that each forwarding route lookup rotates through all the parallel “best” routes. (Parallel routes are defined as routes to the same subnet with the same metrics that only differ by their next hop address.)

Default Values

By default, ip load-sharing is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example turns on load-sharing per destination:

```
(config)# ip load-sharing per-destination
```

The following example disables load-sharing:

```
(config)# no ip load-sharing
```

ip local policy route-map *<map-name>*

Use this command to specify a route-map for local policy routing on the device. This setting is applied to the local network interface. Use the **no** form of this command to return to the default route-map.

Syntax Description

<map-name>	Specify the name of the route-map.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

Before a route map can be specified, it must first be defined using the **route-map** command. See *route-map <map-name> [permit | deny] <sequence number>* on page 439 for more information.

Usage Examples

The following example specifies a route-map entitled myMap for local policy routing:

```
(config)#ip local policy route-map myMap
```

ip mcast-stub helper-address *<ip address>*

Use the **ip mcast-stub helper-address** command to specify an IP address toward which IGMP host reports and leave messages are forwarded. This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub downstream** and **ip mcast-stub upstream** commands. Use the **no** form of this command to return to default.

Syntax Description

<*ip address*>	Specifies the address to which the IGMP host reports and leave messages are forwarded.

Default Values

By default, no helper-address is configured.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

The helper address is configured globally and applies to all multicast-stub downstream interfaces. The address specified may be the next upstream hop or any upstream address on the distribution tree for the multicast source, up to and including the multicast source. The router selects, from the list of multicast-stub upstream interfaces, the interface on the shortest path to the specified address. The router then proxies, on the selected upstream interface (using an IGMP host function), any host joins/leaves received on the downstream interface(s). The router retransmits these reports with addresses set as if the report originated from the selected upstream interface.

For example, if the router receives multiple joins for a group, it will not send any extra joins out the upstream interface. Also, if it receives a leave, it will not send a leave until it is certain that there are no more subscribers on any downstream interface.

Usage Examples

The following example specifies 172.45.6.99 as the helper address:

```
(config)#ip mcast-stub helper-address 172.45.6.99
```

ip multicast-routing

Use the **ip multicast-routing** command to enable the multicast router process. The command does not affect other multicast-related configurations. Use the **no** form of this command to disable. Disabling this command prevents multicast forwarding but does not remove other multicast commands and processes.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables multicast functionality:

```
(config)#ip multicast-routing
```

ip name-server *<server-address1-6>*

Use the **ip name-server** command to designate one or more name servers to use for name-to-address resolution. Use the **no** form of this command to remove any addresses previously specified.

Syntax Description

<server-address1-6>	Specifies up to six name-server addresses.

Default Values

By default, no name servers are specified.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example specifies host 172.34.1.111 as the primary name server and host 172.34.1.2 as the secondary server:

```
(config)#ip name-server 172.341.1.111 172.34.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.34.1.111 172.34.1.2
```

ip policy-class *<policyname>* max-sessions *<number>*

Use the **ip policy-class** command to create an access control policy and enter the access control policy. Use the **no** form of this command to delete an access policy and all the entries contained in it.

> NOTE *Configured access policies will only be active if the* ***ip firewall*** *command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

> CAUTION *Before applying an access control policy to an interface, verify your Telnet connection will not be affected by the policy. If a policy is applied to the interface you are connecting through and it does not allow Telnet traffic, your connection will be lost.*

Syntax Description

<policyname>	Identifies the configured access policy using an alphanumeric descriptor (maximum of 255 characters). All access policy descriptors are case-sensitive.
max-sessions *<number>*	Optional. Configures a maximum number of allowed policy sessions. This number must be within the appropriate range limits. The limits are either 1 to 4000 or 1 to 30,000 (depending on the type of AOS device you are using).

Default Values

By default, all AOS security features are disabled and there are no configured access lists.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

AOS access control policies are used to allow, discard, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded.

The following commands are contained in the **policy-class**:

allow list <*access list names*>
All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>
All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>
All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>
All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload policy** <*access policy name*>
All packets passed by the access list(s) and destined for the interface using the access policy listed will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload policy** <*access policy name*>
All packets passed by the access list(s) and destined for the interface using the access policy listed will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>
All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Usage Examples

Refer to the *Technology Review* (which follows) for command syntax examples.

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:

Enable the security features of the AOS using the **ip firewall** command.

Step 2:

Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a "range." Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a "don't care." For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:

Create an access policy that uses a configured access list. AOS access policies are used to allow, discard, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>

All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>

All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> address <*IP address*> **overload policy** <*access policy name*>

All packets passed by the access list(s) and destined for the interface using the access policy listed will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload policy** <*access policy name*>

All packets passed by the access list(s) and destined for the interface using the access policy listed will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the Ethernet 0/1 interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#access-policy MatchAll
```

ip policy-timeout *<protocol> <range> <port> <seconds>*

Use multiple **ip policy-timeout** commands to customize timeout intervals for protocols (TCP, UDP, ICMP, AHP, GRE, ESP) or specific services (by listing the particular port number). Use the **no** form of this command to return to the default timeout values.

Syntax Description

<protocol> Specifies the data protocol such as ICMP, TCP, UDP, AHP, GRE, or ESP.

<range> Optional. Customizes timeout intervals for a range of TCP or UDP ports.

<port> Specifies the service port to apply the timeout value to; valid only for specifying TCP and UDP services (not allowed for ICMP).

The following is the list of UDP port numbers that may be identified using the text name (in **bold**):

all-ports
biff (Port 512)
bootpc (Port 68)
bootps(Port 67)
discard (Port 9)
dnsix (Port 195)
domain (Port 53)
echo (Port 7)
isakmp (Port 500)
mobile-ip (Port 434)
nameserver (Port 42)
netbios-dgm (Port 138)
netbios-ns (Port 137)
netbios-ss (Port 139)
ntp (Port 123)
pim-auto-rp (Port 496)
rip (Port 520)
snmp (Port 161)
snmptrap (Port 162)
sunrpc (Port 111)
syslog (Port 514)
tacacs (Port 49)
talk (Port 517)
tftp (Port 69)
time (Port 37)
who (Port 513)
xdmcp (Port 177)

The following is the list of TCP port numbers that may be identified using the text name (in **bold**):

all_ports
bgp (Port 179)
chargen (Port 19)
cmd (Port 514)
daytime (Port 13)
discard (Port 9)
domain (Port 53)
echo (Port 7)
exec (Port 512)
kshell (Port 544)
login (Port 513)
lpd (Port 515)
nntp (Port 119)
pim-auto-rp (Port 496)
pop2 (Port 109)
pop3 (Port 110)
smtp (Port 25)
ssh (Port 22)

Syntax Description (Continued)

	finger (Port 79)	**sunrpc** (Port 111)
	ftp (Port 21)	**syslog** (Port 514)
	Optional. **ftp-data** (Port 20)	**tacacs** (Port 49)
	gopher (Port 70)	**talk** (Port 517)
	hostname (Port 101)	**telnet** (Port 23)
	https (443)	**time** (Port 37)
	ident (Port 113)	**uucp** (Port 540)
	irc (Port 194)	**whois** (Port 43)
	klogin (Port 543)	**www** (Port 80)
<seconds>	Wait interval (in seconds) before an active session is closed (valid range: 0 to 4294967295 seconds).	

Default Values

<seconds>	The following default policy timeout intervals apply:
	tcp (600 seconds; 10 minutes)
	udp (60 seconds; 1 minute)
	icmp (60 seconds; 1 minute)
	ahp (60 seconds; 1 minute)
	gre (60 seconds; 1 minute)
	esp (60 seconds; 1 minute)

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 11.1	Added AHP, GRE, and ESP policies.

Usage Examples

The following example creates customized policy timeouts for the following:
Internet traffic (TCP Port 80) timeout 24 hours (86400 seconds)
Telnet (TCP Port 23) timeout 20 minutes (1200 seconds)
FTP (21) timeout 5 minutes (300 seconds)
All other TCP services timeout 8 minutes (480 seconds)

```
(config)#ip policy-timeout tcp www 86400
(config)#ip policy-timeout tcp telnet 1200
(config)#ip policy-timeout tcp ftp 300
(config)#ip policy-timeout tcp all_ports 480
```

The following example creates customized policy timeouts for UDP netbios ports 137 to 139 of 200 seconds and UDP ports 6000 to 7000 of 300 seconds:

```
(config)#ip policy-timeout udp range netbios-ns netbios-ss 200
(config)#ip policy-timeout udp range 6000 7000 300
```

The following example creates a customized policy timeout of 1200 seconds for ESP:

```
(config)#ip policy-timeout esp 1200
```

The following example creates a customized policy timeout of 1200 seconds for GRE:

```
(config)#ip policy-timeout gre 1200
```

The following example creates a customized policy timeout of 1200 seconds for AHP:

```
(config)#ip policy-timeout ahp 1200
```

ip prefix-list *<listname>* description *<"text">*

Use the **ip prefix-list description** command to create and name prefix lists.

Syntax Description

<listname>	Specifies a particular prefix list.
description *<"text">*	Assigns text (set apart by quotation marks) used as a description for the prefix list. Maximum length is 80 characters.

Default Values

No default values are necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command adds a string of up to 80 characters as a description for a prefix list. It also creates the prefix list if a prefix list of that name does not already exist.

Usage Examples

The following example adds a description to the prefix-list **test**:

```
(config)#ip prefix-list test description "An example prefix list"
```

ip prefix-list *<listname>* seq *<sequence#>* [permit | deny] *<network/len>* [le *<le-value>* | ge *<ge-value>*]

Use the **ip prefix-list seq** command to specify a prefix to be matched or a range of mask lengths.

Syntax Description

<listname>	Specifies a particular prefix list.
<sequence#>	Specifies the entry's unique sequence number which determines the processing order. Lower-numbered entries are processed first. Range: 1 to 4,294,967,294.
permit	Permits access to matching entries.
deny	Denies access to matching entries.
<network/len>	Specifies the network number and network mask length.
le *<le-value>*	Specifies the upper end of the range. Range: 0 to 32.
ge *<ge-value>*	Specifies the lower end of the range. Range: 0 to 32.

Default Values

If no ge or le parameters are specified, an exact match is assumed. If only ge is specified, the range is assumed to be from ge-value to 32. If only le is specified, the range is assumed to be from len to le-value.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command specifies a prefix to be matched. Optionally, it may specify a range of mask lengths. The following rule must be followed: len < ge-value ≤ le-value. A prefix list with no entries allows all routes. A route that does not match any entries in a prefix list is dropped. As soon as a route is permitted or denied, there is no further processing of the rule in the prefix list. A route that is denied at the beginning entry of a prefix list will not be allowed, even if it matches a permitting entry further down the list.

Usage Examples

The following example creates a prefix list entry in the prefix list **test** matching only the 10.0.0.0/8 network:

```
(config)#ip prefix-list test seq 5 deny 10.0.0.0/8
```

The following example creates a prefix list entry in the prefix list **test** matching any network of length 24 or less:

```
(config)#ip prefix-list test seq 10 permit 0.0.0.0/0 le 24
```

ip radius source-interface *<interface>*

Use the **ip radius source-interface** command to specify the network-attached storage (NAS) IP address attribute passed with the RADIUS authentication request packet.

Syntax Description

<interface>	Specifies the source interface (in the format **type slot/port**). Type **ip radius source-interface ?** for a complete list of interfaces.

Default Values

By default, no source interface is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

If this value is not defined, the address of the source network interface is used.

Usage Examples

The following example configures the Ethernet 0/1 port to be the source interface:

```
(config)#ip radius source-interface ethernet 0/1
```

ip route *<ip address> <subnet mask> <interface or ip address> <administrative distance>*

Use the **ip route** command to add a static route to the route table. This command can be used to add a default route by entering **ip route 0.0.0.0 0.0.0.0** and specifying the interface or IP address. Use the **no** form of this command to remove a configured static route.

Syntax Description

<ip address>	Specifies the network address (in dotted decimal notation) to add to the route table.
<subnet mask>	Specifies the subnet mask (in dotted decimal notation) associated with the listed network IP address.
<interface or ip address>	Specifies the gateway peer IP address (in dotted decimal notation) or a configured interface in the unit. Use the **ip route interface ?** command to display a complete list of interfaces.
<administrative distance>	Specifies an administrative distance associated with a particular router used to determine the best route when multiple routes to the same destination exist. The smaller the administrative distance the more reliable the route. (Range is 1 to 255.)

Default Values

By default, there are no configured routes in the route table.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	Tunnel added as a supported interface.
Release 11.1	Demand added as a supported interface.

Usage Examples

The following example adds a static route to the **10.220.0.0/16** network through the next-hop router **192.22.45.254** and a default route to **175.44.2.10**:

```
(config)#ip route 10.220.0.0 255.255.0.0 192.22.45.254
(config)#ip route 0.0.0.0 0.0.0.0 175.44.2.10
```

ip routing

Use the **ip routing** command to enable the AOS IP routing functionality. Use the **no** form of this command to disable IP routing.

Syntax Description

No subcommands.

Default Values

By default, IP routing is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the AOS IP routing functionality:

```
(config)#ip routing
```

ip rtp firewall-traversal [policy-timeout *<seconds>*]

Use the **ip rtp firewall-traversal** command to enable dynamic firewall traversal capability for RTP-based traffic, allowing deep packet inspection of SDP packets to occur so RTP will correctly traverse NAT in the firewall. This will open the proper ports dynamically for the RTP traffic.

Syntax Description

policy-timeout *<seconds>*	Optional. Specifies timeout period allowed for inactive RTP sessions to remain in the firewall. Range is 1 to 4,294,967,295.

Default Values

By default, the policy timeout period is 45 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Functional Notes

If this value is not defined, the address of the source network interface is used.

Usage Examples

The following example enables dynamic firewall traversal and sets the policy timeout period at **60** seconds:

```
(config)#ip rtp firewall-traversal policy-timeout 60
```

ip scp server

Use the **ip scp server** to enable the secure copy (SCP) server. SCP is a more secure form of the older Berkley r-tool RCP or remote copy. It allows an SCP client to send or receive files to/from the unit. SCP relies on Secure Shell (SSH) for authentication and encryption of the data transfer.

Syntax Description

No subcommands.

Default Values

By default, the secure copy server is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example enables the secure copy server:

```
(config)#ip scp server
```

ip sip [database local | location] *<username> <ip address>*

Use the **ip sip database local** command to store the database of SIP usernames across a reboot. Use the **ip sip location** command to configure the SIP location database parameters. Use the **no** form of the **ip sip location** command to return to the defaults.

Syntax Description

database local	Stores the database on the local machine.
location	Sets the parameters for the location database.
<*username*>	Specifies the username to use.
<*ip address*>	Specifies the IP address for the SIP server.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies an IP SIP location of 192.33.5.99 for a user named 2001:

```
(config)#ip sip location 2001 192.33.5.99
```

ip sip proxy

Use the **ip sip proxy** command to enable or disable the proxy server.

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables the proxy server:

```
(config)#ip sip proxy
```

ip sip registrar [authenticate | default-expires | max-expires | min-expires | realm] <*timevalue*>

Use the **ip sip registrar** command to configure the registrar server. Use the **no** form of the **ip sip registrar authenticate** command to disable the registrar server.

Syntax Description

authenticate	Specify authentication is required on server upon registration.
default-expires	Specify the default expiration period.
max-expires	Specify the maximum expiration period. Seconds: 0 to 2,592,000.
min-expires	Specify the minimum expiration period. Seconds: 0 to 2,592,000.
realm	Specify string for authentication parameter.
<*timevalue*>	Specify time in seconds.

Default Values

By default, the registrar server is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the default expiration to 5 seconds:

```
(config)#ip sip registrar default-expires 5
```

The following example sets the realm string:

```
(config)#ip sip registrar realm voice.adtran.com
```

ip snmp agent

Use the **ip snmp agent** command to enable the Simple Network Management Protocol (SNMP) agent.

Syntax Description

No subcommands.

Default Values

By default, the SNMP agent is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Allows a MIB browser to access standard MIBs within the product. This also allows the product to send traps to a trap management station.

Usage Examples

The following example enables the IP SNMP agent:

```
(config)#ip snmp agent
```

ip sntp source-interface *<interface>*

The **ip sntp source-interface** command to use the specified interface’s IP address as the source IP address for SNTP traffic transmitted by the unit. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<interface>	Specifies the interface to be used as the source IP address for SNTP traffic.Type **ip sntp source-interface?** for a complete list of valid interfaces.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for SNTP traffic:

```
(config)#ip sntp source-interface loopback
```

ip [ssh-server *<port>* | telnet-server *<port>*]

Use the this command to specify alternate transmission control protocol (TCP) ports for secure shell (SSH) and Telnet servers. Use the **no** form of this command to return to default settings.

Syntax Description

ssh server *<port>*	Configures the SSH server to listen on an alternate TCP port.
telnet server *<port>*	Configures the Telnet server to listen on an alternate TCP port.

Default Values

By default, the SSH server listens on TCP port 22 and Telnet listens on TCP port 23.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

SSH is a newer version of Telnet which allows you to run command line and graphical applications (as well as transfer files) over an encrypted connection.

Usage Examples

The following example configures the Telnet server to listen on TCP port **2323** instead of the default port **23**:

```
(config)#ip telnet-server 2323
```

The following example configures the SSH server to listen on TCP port **2200** instead of the default port **22**:

```
(config)#ip ssh-server 2200
```

To return to the default settings, use the **no** version of the command. For example:

```
(config)#no ip ssh-server 2200
```

ip subnet-zero

The **ip subnet-zero** command is the default operation and cannot be disabled. This command signifies the router's ability to route to subnet-zero subnets.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example **subnet-zero** is enabled:

```
(config)#ip subnet-zero
```

ip tftp source-interface *<interface>*

Use the **ip tftp source-interface** command to use the specified interface's IP address as the source IP address for TFTP traffic transmitted by the unit. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<*interface*>	Specifies the interface to be used as the source IP address for TFTP traffic.

Default Values

No default value is necessary for this command.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for TFTP traffic:

```
(config)#ip tftp source-interface loopback 1
```

line [console | telnet | ssh] *<line-number> <ending number>*

Use the **line** command to enter the line configuration for the specified console, Telnet, or secure shell (SSH) session. Refer to the sections *Line (Console) Interface Config Command Set* on page 470, *Line (Telnet) Interface Config Command Set* on page 491, and *Line (SSH) Interface Config Command Set* on page 483 for information on the subcommands.

Syntax Description

console	Enters the configuration mode for the DB-9 (female) **CONSOLE** port located on the rear panel of the unit. Refer to the sections *Line (Console) Interface Config Command Set* on page 816 for information on the subcommands found in that command set.
telnet	Enters the configuration mode for Telnet session(s), allowing you to configure for remote access. Refer to the section *Line (Telnet) Interface Config Command Set* on page 491 for information on the subcommands found in that command set.
ssh	Enters the configuration mode for SSH. Refer to the section *Line (SSH) Interface Config Command Set* on page 483 for information on the subcommands found in that command set.
<line-number>	Specifies the starting session to configure for remote access (valid range for console: 0; valid range for Telnet and SSH: 0 to 4). If configuring a single Telnet or SSH session, enter the session number and leave the *<ending number>* field blank.
<ending number>	Optional. Specifies the last Telnet or SSH session to configure for remote access (valid range: 0 to 4). For example, to configure all available Telnet sessions, enter **line telnet 0 4**.

Default Values

By default, the AOS line console parameters are configured as follows:

Data Rate: 9600
Data bits: 8
Stop bits: 1
Parity Bits: 0
No flow control

By default, there are no configured Telnet or SSH sessions.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include SSH.

Usage Examples

The following example begins the configuration for the **CONSOLE** port located on the rear of the unit:

```
(config)#line console 0
(config-con0)#
```

The following example begins the configuration for all available Telnet sessions:

```
(config)#line telnet 0 4
(config-telnet0-4)#
```

The following example begins the configuration for all available SSH sessions:

```
(config)#line ssh 0 4
(config-ssh0-4)#
```

lldp [minimum-transmit-interval | reinitialization-delay | transmit-interval | ttl-multiplier] *<numeric value>*

Use the **lldp** command to configure global settings that control the way LLDP functions.

Syntax Description

minimum-transmit-interval	Defines the minimum amount of time between transmission of LLDP frames (in seconds).
reinitialization-delay	Defines the minimum amount of time to delay after LLDP is disabled on a port before allowing transmission of additional LLDP frames on that port (in seconds).
transmit-interval	Defines the delay between LLDP frame transmission attempts during normal operation (in seconds).
ttl-multiplier	Defines the multiplier to be applied to the transmit interval to compute the time-to-live for data sent in an LLDP frame.
<numeric value>	Specifies the interval, delay, or multiplier.

Default Values

By default, **minimum-transmit-interval** = 2 seconds (valid range: 1 through 8192); **reinitialization-delay** = 2 seconds (valid range 1 through 10); **transmit-interval** = 30 seconds (valid range 5 through 32,768); and **ttl-multiplier** = 4 (valid range 2 through 10).

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

Once a device receives data from a neighboring device in an LLDP frame, it will retain that data for a limited amount of time. This amount of time is called time-to-live, and it is part of the data in the LLDP frame. The time-to-live transmitted in the LLDP frame is equal to the transmit interval multiplied by the TTL multiplier.

Usage Examples

The following example sets the LLDP minimum transmit interval to 10 seconds:

```
(config)#lldp minimum-transmit-interval 10
```

The following example sets the LLDP reinitialization delay to 5 seconds:

```
(config)#lldp reinitialization-delay 5
```

The following example sets the LLDP transmit interval to 15 seconds:

```
(config)#lldp transmit-interval 15
```

The following example sets the LLDP TTL multiplier to 2 and the time-to-live for all LLDP frames transmitted from this unit to 30 seconds;

```
(config)#lldp transmit-interval 15
(config)#lldp ttl-multiplier 2
```

logging console

Use the **logging console** command to enable the AOS to log events to all consoles. Use the **no** form of this command to disable console logging.

Syntax Description

No subcommands.

Default Values

By default, logging console is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables the AOS to log events to all consoles:

```
(config)#logging console
```

logging email address-list *<email address>* ; *<email address>*

Use the **logging email address-list** command to specify one or more email addresses that will receive notification when an event matching the criteria configured using the **logging email priority-level** command is logged by the AOS. Refer to *logging email priority-level [error | fatal | info | notice | warning]* on page 421 for more information. Use the **no** form of this command to remove a listed address.

Syntax Description

<email address>	Specifies the complete email address to use when sending logged messages. (This field allows up to 256 characters.) Enter as many email addresses as desired, placing a semi-colon (;) between addresses.

Default Values

By default, there are no configured logging email addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies three email addresses to use when sending logged messages:

```
(config)#logging email address-list
admin@adtranemail.com;ntwk@adtranemail.com;support@adtranemail.com
```

logging email exception-report address-list *<email address>*; *<email address>*

Use the **logging email exception-report address-list** command to specify one or more email addresses to receive an exception report for use in troubleshooting. Use the **no** form of this command to remove a listed address.

Syntax Description

<email address>	Specifies the complete email address to use when sending exception reports. (This field allows up to 256 characters.) Enter as many email addresses as desired, placing a semi-colon (;) between addresses.

Default Values

By default, there are no configured logging email addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

When AOS experiences an exception it will generate a file with detailed information that ADTRAN's Technical Support can use to diagnose the problem, This command allows the unit to email the exception report to a list of addresses upon rebooting after the exception. This command should be used in conjunction with the other logging email commands. Refer to *logging email address-list <email address> ; <email address>* on page 418, *logging email on* on page 420, *logging email priority-level [error | fatal | info | notice | warning]* on page 421, *logging email receiver-ip <ip address>* on page 422, *logging email sender* on page 423, and *logging email source-interface <interface>* on page 424 for more information.

Usage Examples

The following example will enable exception report forwarding to **john.doe@company.com** using the **1.1.1.1** SMTP email server:

```
(config)#logging email on
(config)#logging email receiver-ip 1.1.1.1
(config)#logging email exception-report address-list john.doe@company.com
```

logging email on

Use the **logging email on** command to enable the AOS email event notification feature. Use the **logging email address-list** command to specify email address(es) that will receive notification when an event matching the criteria configured using the **logging email priority-level** command is logged by the AOS. Refer to *logging email priority-level [error | fatal | info | notice | warning]* on page 421 for more information. Use the **no** form of this command to disable the email notification feature.

Syntax Description

No subcommands.

Default Values

By default, email event notification is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The domain name is appended to the sender name when sending event notifications. Refer to the command *ip domain-name <name>* on page 363 for related information.

Usage Examples

The following example enables the AOS email event notification feature:

```
(config)#logging email on
```

logging email priority-level [error | fatal | info | notice | warning]

Use the **logging email priority-level** command to set the threshold for events sent to the addresses specified using the **logging email address-list** command. All events with the specified priority or higher will be sent to all addresses in the list. The **logging email on** command must be enabled. Refer to *logging email address-list <email address> ; <email address>* on page 418 and *logging email on* on page 420 for related information. Use the **no** form of this command to return to the default priority.

Syntax Description

Sets the minimum priority threshold for sending messages to email addresses specified using the **logging email address-list** command.

The following priorities are available (ranking from lowest to highest):

error	Logs events with **error** and **fatal** priorities.
fatal	Logs only events with a **fatal** priority.
info	Logs all events.
notice	Logs events with **notice**, **warning**, **error**, and **fatal** priorities.
warning	Logs events with **warning**, **error**, and **fatal** priorities.

Default Values

By default, the **logging email priority-level** is set to **warning**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sends all messages with **warning** level or greater to the email addresses listed using the **logging email address-list** command:

```
(config)#logging email priority-level warning
```

logging email receiver-ip *<ip address>*

Use the **logging email receiver-ip** command to specify the IP address of the email server to use when sending notification that an event matched the criteria configured using the **logging email priority-level** command. Refer to *logging email priority-level [error | fatal | info | notice | warning]* on page 421 for related information. Use the **no** form of this command to remove a configured address.

Syntax Description

<ip address>	Specifies the IP address (in dotted decimal notation) of the mail server to use when sending logged messages.

Default Values

By default, there are no configured email server addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies an email server (with address 172.5.67.99) to use when sending logged messages:

```
(config)#logging email receiver-ip 172.5.67.99
```

logging email sender

Use the **logging email sender** command to specify the sender in an outgoing email message. This name will appear in the **From** field of the receiver's inbox. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example sets a sender for outgoing messages:

```
(config)#logging email sender myUnit@myNetwork.com
```

logging email source-interface *<interface>*

Use the **logging email source-interface** command to use the specified interface's IP address as the source IP address for email messages transmitted by the unit. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<*interface*>	Specifies the interface to be used as the source IP address for email messages.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

The following example configures the unit to use the **loopback 1** interface as the source IP for email messages:

```
(config)#logging email source-interface loopback 1
```

logging facility *<facility type>*

Use the **logging facility** command to specify a syslog facility type for the syslog server. Error messages meeting specified criteria are sent to the syslog server. For this service to be active, you must enable log forwarding. Refer to *logging forwarding on* on page 427 for related information. Facility types are described under *Functional Notes* below. Use the **no** form of this command to return it to its default setting.

Syntax Description

<facility type>	Specifies the syslog facility type (refer to *Functional Notes* below).

Default Values

The default value is local7.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The following is a list of all the valid facility types:

auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0 - local7	Reserved for locally-defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9 - sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Usage Examples

The following example configures the syslog facility to the cron facility type:

```
(config)#logging facility cron
```

logging forwarding on

Use the **logging forwarding on** command to enable the AOS syslog event feature. Use the **logging forwarding priority-level** command to specify the event matching the criteria used by the AOS to determine whether a message should be forwarded to the syslog server. Refer to *logging forwarding priority-level [error | fatal | info | notice | warning]* on page 428 for related information. Use the **no** form of this command to disable the syslog event feature.

Syntax Description

No subcommands.

Default Values

By default, syslog event notification is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the AOS syslog event feature:

```
(config)#logging forwarding on
```

logging forwarding priority-level [error | fatal | info | notice | warning]

Use the **logging forwarding priority-level** command to set the threshold for events sent to the configured syslog server specified using the **logging forwarding receiver-ip** command. All events with the specified priority or higher will be sent to all configured syslog servers. Refer to *logging email priority-level [error | fatal | info | notice | warning]* on page 421 for more information. Use the **no** form of this command to return to the default priority.

Syntax Description

Sets the minimum priority threshold for sending messages to the syslog server specified using the **logging forwarding receiver-ip** command.

The following priorities are available (ranking from lowest to highest):

error	Logs events with **error** and **fatal** priorities.
fatal	Logs only events with a **fatal** priority.
info	Logs all events.
notice	Logs events with **notice**, **warning**, **error**, and **fatal** priorities.
warning	Logs events with **warning**, **error**, and **fatal** priorities.

Default Values

By default the **logging forwarding priority-level** is set to **warning**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sends all messages with **warning** level or greater to the syslog server listed using the **logging forwarding receiver-ip** command.

```
(config)#logging forwarding priority-level warning
```

logging forwarding receiver-ip *<ip address>*

Use this **logging forwarding receiver-ip** command to specify the IP address of the syslog server to use when logging events that match the criteria configured using the **logging forwarding priority-level** command. Enter multiple **logging forwarding receiver-ip** commands to develop a list of syslog servers to use. Refer to *logging forwarding priority-level [error | fatal | info | notice | warning]* on page 428 for related information. Use the **no** form of this command to remove a configured address.

Syntax Description

<ip address>	Specifies the IP address (in dotted decimal notation) of the syslog server to use when logging messages.

Default Values

By default, there are no configured syslog server addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a syslog server (with address **172.5.67.99**) to use when logging messages:

```
(config)#logging forwarding receiver-ip 172.5.67.99
```

logging forwarding source-interface *<interface>*

Use the **logging forwarding source-interface** command to configure the specified interface's IP address as the source IP address for the syslog server to use when logging events. Use the **no** form of this command if you do not wish to override the normal source IP address.

Syntax Description

<*interface*>	Specifies the interface to be used as the source IP address for event log traffic. Type **logging forwarding source-interface?** for a complete list of valid interfaces.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command allows you to override the *sender* field in the IP packet. If you have multiple interfaces in your unit, changing the *sender* tells the receiver where to send replies. This functionality can also be used to allow packets to get through firewalls that would normally block the flow.

Usage Examples

configures the unit to use the **loopback 1** interface as the source IP for event log traffic:

```
(config)#logging forwarding source-interface loopback 1
```

mac address-table aging-time *<aging time>*

Use the **mac address-table aging-time** command to set the length of time dynamic MAC addresses remain in the switch or bridge forwarding table. Use the **no** form of this command to reset this length to its default.

Syntax Description

<aging time>	Set an aging time (in seconds) from 10 to 1,000,000. Set to 0 to disable the timeout.

Default Values

By default, the aging time is 300 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the aging time to 10 minutes:

```
(config)#mac address-table aging-time 600
```

mac address-table static *<mac address>* bridge *<bridge id>* interface *<interface>*

Use the **mac address-table static** command to insert a static MAC address entry into the bridge forwarding table. Use the **no** form of this command to remove an entry from the table.

Syntax Description

<mac address>	Specifies a valid 48-bit MAC address.
<bridge>	Specifies a valid bridge interface ID.
interface	Specifies the interface. Type **mac address-table static bridge interface ?** for a complete list of valid interfaces.
<interface>	Specifies a valid slot/port interface ID.

Default Values

By default, there are no static entries configured.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example adds a static MAC address to PPP 1 on bridge 4:

```
(config)#mac address-table static 00:A0:C8:00:00:01 bridge 4 interface ppp 1
```

power-supply shutdown automatic

Use the **power-supply shutdown automatic** command to enable the power supplies to automatically shut down when the unit temperature exceeds the maximum operating temperature. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables the power supplies to shut down automatically if the temperature gets too high:

```
(config)#power-supply shutdown automatic
```

qos map *<mapname> <sequence number>*

Use the **qos map** command to activate the QoS Map Command Set (which allows you to create and/or edit a QoS map). For details on specific commands, refer to the section *Quality of Service (QoS) Map Commands* on page 1163. Use the **no** form of this command to delete a map entry.

Syntax Description

<mapname>	Specifies the QoS map name.
<sequence number>	Specifies a number (valid range: 0 to 65,535) to differentiate this QoS map and to assign match order.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

A QoS policy is defined using a QoS map. The QoS map is a named list with sequenced entries. An entry contains a single match reference and one or more actions (**priority**, **set**, or **both**). Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign match order.

Once created, a QoS map must be applied to an interface (using the **qos-policy out** *<map-name>* command) in order to actively process traffic. Any traffic for the interface that is not sent to the priority queue is sent using the default queuing method for the interface (such as weighted fair queuing).

Usage Examples

The following example demonstrates basic settings for a QoS map and assigns a map to the Frame Relay interface:

```
>enable
#config terminal
(config)#qos map VOICEMAP 10
(config-qos-map)#match precedence 5
(config-qos-map)#priority 512
(config-qos-map)#exit
(config)#interface fr 1
(config-fr 1)#qos-policy out VOICEMAP
```

radius-server

Use the **radius-server** command to configure several global RADIUS parameters. Most of these global defaults can be overridden on a per-server basis.

Variations of this command include the following:

radius-server challenge-noecho
radius-server deadtime <*minutes*>
radius-server enable-username <*name*>
radius-server key <*key*>
radius-server retry <*attempts*>
radius-server timeout <*seconds*>

Syntax Description

challenge-noecho	Turns off echoing of user challenge-entry. When echo is turned on, users see the text of the challenge as they type responses. Enabling this option hides the text as it is being entered.
deadtime <*minutes*>	Specifies how long a RADIUS server is considered dead once a timeout occurs. The server will not be tried again until after the deadtime expires.
enable-username <*name*>	Specifies a username to be used for enable authentication.
key <*key*>	Specifies the shared key to use with a RADIUS server.
retry <*attempts*>	Specifies how many attempts to make on a RADIUS server before marking it dead.
timeout <*seconds*>	Specifies how long to wait for a RADIUS server to respond to a request.

Default Values

challenge-noecho	By default, echo is turned on.
deadtime	1 minute
key	No default
retry	3 attempts
timeout	5 seconds
enable-username	$enab15$

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 7.1	Added **enable-username** selection.

Functional Notes

RADIUS servers (as defined with the **radius-server** command) may have many optional parameters. However, they are uniquely identified by their addresses and ports. Port values default to 1812 and 1813 for authorization and accounting, respectively. If a server is added to a named group but is not defined by a **radius-server** command, the server is simply ignored when accessed. Empty server lists are not allowed. When the last server is removed from a list, the list is automatically deleted.

Usage Examples

The following example shows a typical configuration of these parameters:

```
(config)#radius-server challenge-noecho
(config)#radius-server deadtime 10
(config)#radius-server timeout 2
(config)#radius-server retry 4
(config)#radius-server key my secret key
```

radius-server host

Use the **radius-server host** to specify the parameters for a remote RADIUS server. At a minimum, the address (IP or DNS name) of the server must be given. The other parameters are also allowed and (if not specified) will take default values or fall back on the global RADIUS server's default settings.

Syntax Description

acct-port <*port#*>	Sends accounting requests to this remote port.
auth-port <*port#*>	Sends authentication requests to this remote port.
retry <*attempts*>	Retries server after timeout this number of times (uses RADIUS global setting if not given).
timeout <*seconds*>	Waits for a response this number of seconds (uses RADIUS global setting if not given).
key <*key*>	Defines the shared key with the RADIUS server (uses RADIUS global setting if not given). Note that the key must appear last on the input line since it reads the rest of the line beyond the **key** keyword.
key encrypted <*key*>	Defines an encrypted shared key with the RADIUS server (uses RADIUS global setting if not given). Note that the key must appear last on the input line since it reads the rest of the line beyond the **key** keyword.

Default Values

By default, **acct-port** is set to 1813 and **auth-port** is set to 1812.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command was expanded to include the **key encrypted** command.

Usage Examples

The following example shows a typical configuration of these parameters:

```
(config)#radius-server host 1.2.3.4
(config)#radius-server host 3.3.1.2 acct-port 1646 key my key
```

route-map *<map-name>* [permit | deny] *<sequence number>*

Use the **route-map** command to create a route map and enter the Route Map Configuration command set. A route map is a type of filter that matches various attributes and then performs actions on the way the route is redistributed. Use the **no** form of this command to delete a route map.

Syntax Description

<map-name>	Specifies a name for the route map.
permit	Redistributes routes matching the route map attributes.
deny	Specifies not to redistribute routes matching the route map attributes.
<sequence number>	Specifies a sequence number of this route entry. Range is 1 to 4,294,967,295.

Default Values

By default, no route maps are defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

Route maps can be assigned to a neighbor using the **route-map** command in the BGP Neighbor command set. See *route-map <map-name> [in | out]* on page 1107 for more information.

Usage Examples

The following example creates the route map, specifies that routes matching its criteria will be denied, and assigns a sequence number of 100:

```
(config)#route-map MyMap deny 100
(config-route-map)#
```

You can then define the attributes of the route map from the Route Map Configuration Command set. Enter a **?** at the **(config-route-map)#** prompt to explore the available options.

router bgp

Use the **router bgp** command to enter the BGP Configuration mode. Refer to the BGP Configuration Command section for more information.

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example uses the **router bgp** command to enter the BGP Configuration mode:

```
(config)#router bgp
(config-bgp)#
```

Technology Review

The following AOS BGP-related guidelines may help guide decisions made during basic BGP implementation.

Ignore route if next hop is unreachable.

Prefer route with largest weight (only used in the local router, set by applying route maps to set this value on desired inbound updates).

Prefer route with largest local preference.

Prefer route injected by this router via network command.

Prefer route with shortest AS_PATH.

Prefer route with lowest origin type. Routes originally injected by the network command or aggregation (IGP) have a lower origin type than those originally injected by redistribution into BGP.

Prefer routes with lowest MED value.

Before the route is installed into the route table (forwarding table), a check is made of other sources that may have information about the same subnet (static routes, IGP, etc.) The route with the lowest administrative distance is installed.

router ospf

Use the **router ospf** command to activate OSPF in the router and to enter the OSPF Configuration mode. Refer to the section *Router (OSPF) Configuration Command Set* on page 1114 for more information. Use the **no** form of this command to disable OSPF routing.

Syntax Description

No subcommands.

Default Values

By default, OSPF is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The AOS can be configured to use OSPF with the firewall enabled (using the **ip firewall** command). To do this, configure the OSPF networks as usual, specifying which networks the system will listen for and broadcast OSPF packets to. Refer to *ip firewall* on page 365 for more information.

To apply stateful inspection to packets coming into the system, create a policy class that describes the type of action desired and then associate that policy class to the particular interface (refer to *ip policy-class <policyname> max-sessions <number>* on page 390). The firewall is intelligent and will only allow OSPF packets that were received on an OSPF configured interface. No modification to the policy class is required to allow OSPF packets into the system.

Usage Examples

The following example uses the **router ospf** command to enter the OSPF Configuration mode:

```
(config)#router ospf
```

router pim-sparse

Use the **router pim-sparse** command to globally enable protocol-independent multicast (PIM) on the unit and to enter the PIM Sparse Configuration mode. Refer to the section *Router (PIM Sparse) Configuration Command Set* on page 834 for more information on the subcommands for PIM Sparse Configuration mode.

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Functional Notes

Additional commands for PIM are found in the related interface configuration modes. See the **ip pim-sparse** commands in sections such as *Ethernet Interface Configuration Command Set* on page 527, *Frame Relay Sub-Interface Config Command Set* on page 714, *HDLC Command Set* on page 782, *Loopback Interface Configuration Command Set* on page 846, *PPP Interface Configuration Command Set* on page 883, *Tunnel Configuration Command Set* on page 967, and *VLAN Interface Config Command Set* on page 668 for more information.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example uses the **router pim-sparse** command to enter the PIM Sparse Configuration mode:

```
(config)#router pim-sparse
(config-pim-sparse)#
```

router rip

Use the **router rip** command to enter the RIP Configuration mode. Refer to the section *Router (RIP) Configuration Command Set* on page 1134 for more information.

Syntax Description

No subcommands.

Default Values

No default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example uses the **router rip** command to enter the RIP Configuration mode:

```
(config)#router rip
(config-rip)#
```

Technology Review

The RIP protocol is based on the Bellham-Ford (distance-vector) algorithm. This algorithm provides that a network will converge to the correct set of shortest routes in a finite amount of time, provided that:

Gateways continuously update their estimates of routes.
Updates are not overly delayed and are made on a regular basis.
The radius of the network is not excessive.
No further topology changes take place.

RIP is described in RFC 1058 (Version 1) and updated in RFCs 1721, 1722, and 1723 for Version 2. Version 2 includes components that ease compatibility in networks operating with RIP V1.

All advertisements occur on regular intervals (every 30 seconds). Normally, a route that is not updated for 180 seconds is considered dead. If no other update occurs in the next 60 seconds for a new and better route, the route is flushed after 240 seconds. Consider a connected route (one on a local interface). If the interface fails, an update is immediately triggered for that route only (advertised with a metric of 16).

Now consider a route that was learned and does not receive an update for 180 seconds. The route is marked for deletion, and even if it was learned on an interface, a poisoned (metric =16) route should be sent by itself immediately and during the next two update cycles with the remaining normal split horizon update routes. Following actual deletion, the poison reverse update ceases. If an update for a learned route is not received for 180 seconds, the route is marked for deletion. At that point, a 120-second garbage collection (GC) timer is started. During the GC timer period, expiration updates are sent with the metric for the timed-out route set to 16.

If an attached interface goes down, the associated route is immediately (within the same random five-second interval) triggered. The next regular update excludes the failed interface. This is the so-called first hand knowledge rule. If a gateway has first hand knowledge of a route failure (connected interfaces) or reestablishment, the same action is taken. A triggered update occurs, advertising the route as failed (metric = 16) or up (normal metric) followed by the normal scheduled update.

The assumption here is that if a gateway missed the triggered update, it will eventually learn from another gateway in the standard convergence process. This conserves bandwidth.

RIP-Related Definitions:

Route	A description of the path and its cost to a network.
Gateway	A device that implements all or part of RIP (a router).
Hop	A metric that provides the integer distance (number of intervening gateways) to a destination network gateway.
Advertisement	A broadcast or multicast packet to port 520 that indicates the route for a given destination network.
Update	An advertisement sent on a regular 30-second interval including all routes exclusive of those learned on an interface.

service password-encryption

Use the **service password-encryption** command to turn on global password protection. Use the **no** form of this command to return to default settings.

CAUTION *If you need to go back to a previous revision of the code (e.g., AOS Revision 10), this command must be disabled first. Once the service is disabled, all necessary passwords must be re-entered so that they are in the clear text form. If this is not done properly, you will not be able to log back in to the unit after you revert to a previous revision that does not support password encryption.*

Syntax Description

No subcommands.

Default Values

By default, global password protection is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

When enabled, all currently configured passwords are encrypted. Also, any new passwords are encrypted after they are entered. Password encryption is applied to all passwords, including passwords for username, enable, Telnet/console, PPP, BGP, and authentication keys. When passwords are encrypted, unauthorized persons cannot view them in configuration files since the encrypted form of the password is displayed in the running-config. While this provides some level of security, the encryption method used with password encryption is not a strong form of encryption so you should take additional network security measures.

NOTE *You cannot recover a lost encrypted password. You must erase the startup-config and set a new password.*

Usage Examples

The following example enables password encryption for all passwords on the unit:

```
(config)#service password-encryption
```

snmp-server chassis-id *<id string>*

Use the **snmp-server chassis-id** command to specify an identifier for the Simple Network Management Protocol (SNMP) server. Use the **no** form of this command to return to the default value.

Syntax Description

<id string>	Identifies the product using an alphanumeric string (up to 32 characters in length).

Default Values

By default, the **snmp-server chassis-id** is set to **Chassis ID**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures a chassis ID of **A432692**:

```
(config)#snmp-server chassis-id A432692
```

snmp-server community *<community>* view *<viewname>* [ro | rw] *<listname>*

Use the **snmp-server community** command to specify a community string to control access to the Simple Network Management Protocol (SNMP) information. Use the **no** form of this command to remove a specified community.

Syntax Description

<community>	Specifies the community string (a password to grant SNMP access).
view *<viewname>*	Optional. Specifies a previously defined view. Views define objects available to the community. For information on creating a new view, see *snmp-server view <viewname> <oidtree> [excluded | included]* on page 455.
ro	Optional. Keyword to grant read-only access, allowing retrieval of MIB objects.
rw	Optional. Keyword to grant read-write access, allowing retrieval and modification of MIB objects.
<listname>	Optional. Specifies an access-control list name used to limit access. Refer to *ip access-list extended <listname>* on page 344 and *ip access-list standard <listname> [permit | deny] <ip address>* on page 350 for more information on creating access-control lists.

Default Values

By default, there are no configured SNMP communities.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	**view** *<viewname>* option added.

Usage Examples

The following example specifies a community named **MyCommunity**, specifies a previously defined view named **blockinterfaces**, and assigns read-write access:

```
(config)#snmp-server community MyCommunity view blockinterfaces rw
```

snmp-server contact [email | pager | phone] *<number>*

Use the **snmp-server contact** command to specify the email address, pager number, or phone number. Use the **no** form of this command to remove a configured contact.

Syntax Description

email	Specifies email address for the SNMP server contact.
pager	Specifies pager number for the SNMP server contact.
phone	Specifies phone number for the SNMP server contact.
<*number*>	Identifies the contact (up to 32 characters in length).

Default Values

No default values necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example specifies **6536999** for the pager number:

```
(config)#snmp-server contact pager 6536999
```

snmp-server contact *<"string">*

Use the **snmp-server contact** command to specify the SNMP sysContact string. Use the **no** form of this command to remove a configured contact.

Syntax Description

<"string">	Populates the sysContact string using an alphanumeric string enclosed in quotation marks (up to 32 characters in length).

Default Values

By default, the **snmp-server contact** is set to **Customer Service**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies **Network Administrator x4000** for the sysContact string:

```
(config)#snmp-server contact "Network Administrator x4000"
```

snmp-server enable traps *<trap type>* [snmp]

Use the **snmp-server enable traps** command to enable all Simple Network Management Protocol (SNMP) traps available on your system or specified using the *<trap type>* option. Use multiple **snmp-server enable traps** to enable multiple trap types. Use the **no** form of this command to disable traps (or the specified traps).

Syntax Description

<trap type>	Specifies the type of notification trap to enable. Leaving this option blank enables ALL system traps.
snmp	Optional. Enables a subset of traps specified in RFC1157. The following traps are supported: coldStart warmStart linkUp linkDown authenticationFailure

Default Values

By default, there are no enabled traps.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the SNMP traps:

```
(config)#snmp-server enable traps snmp
```

snmp-server host *<address>* traps *<community> <trap type>* [snmp]

Use the **snmp-server host traps** command to specify traps sent to an identified host. Use multiple **snmp-server host traps** commands to specify all desired hosts. Use the **no** form of this command to return to the default value.

Syntax Description

<address>	Specifies the IP address of the SNMP host that receives the traps.
<community>	Specifies the community string (used as a password) for authorized agents to obtain access to SNMP information.
<trap type>	Specifies the type of notification trap to enable. Leaving this option blank enables ALL system traps.
snmp	Optional. Enables a subset of traps specified in RFC1157. The following traps are supported: coldStart warmStart linkUp linkDown authenticationFailure

Default Values

By default, there are no hosts or traps enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sends all SNMP traps to the host at address **190.3.44.69** and community string **My Community**:

```
(config)#snmp-server host 190.3.44.69 traps My Community snmp
```

snmp-server host *<address>* **traps version** *<version> <community> <trap type>* **[snmp]**

Use the **snmp-server host traps version** command to specify traps sent to an identified host. Use multiple **snmp-server host traps version** commands to specify all desired hosts. Use the **no** form of this command to return to the default value.

Syntax Description

<address>	Specifies the IP address of the SNMP host that receives the traps.
<version>	Specifies the SNMP version as one of the following: 1 - SNMPv1 2C - SNMPv2C
<community>	Specifies the community string (used as a password) for authorized agents to obtain access to SNMP information.
<trap type>	Specifies the type of notification trap to enable. Leaving this option blank enables ALL system traps.
snmp	Optional. Enables a subset of traps specified in RFC1157. The following traps are supported: coldStart warmStart linkUp linkDown authenticationFailure

Default Values

By default, there are no hosts or traps enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sends all SNMP traps to the host at address **190.3.44.69** and community string **My Community** using SNMPv2C:

```
(config)#snmp-server host 190.3.44.69 traps version 2c My Community snmp
```

snmp-server location *<"string">*

Use the **snmp-server location** command to specify the Simple Network Management Protocol (SNMP) system location string. Use the **no** form of this command to return to the default value.

Syntax Description

<"string">	Populates the system location string using an alphanumeric string enclosed in quotation marks (up to 32 characters in length).

Default Values

By default, the **snmp-server location** is set to **ADTRAN**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a location of **5th Floor Network Room**:

```
(config)#snmp-server location "5th Floor Network Room"
```

snmp-server source-interface *<interface>*

Use the **snmp-server source-interface** command to tell the AOS the interface type from which to expect the SNMP traps to originate. All SNMP originated packets (including traps and get/set requests) will use the designated interface's IP address. Use the **no** form of this command to remove specified interfaces.

Syntax Description

<interface>	Specifies the physical interface that should originate SNMP traps. Enter **snmp-server trap-source ?** for a complete list of valid interfaces.

Default Values

By default, there are no trap-source interfaces defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example specifies that the Ethernet interface (**ethernet 0/1**) should be the source for all SNMP traps and get/set requests:

```
(config)#snmp-server source-interface ethernet 0/1
```

snmp-server view *<viewname>* *<oidtree>* [excluded | included]

Use the **snmp-server view** command to create or modify a Simple Network Management Protocol (SNMP) view entry. Use the **no** form of this command to remove an entry.

Syntax Description

<viewname>	Specifies a label for the view record being created. The name is a record reference.
<oidtree>	Specifies the object identifier (oid) to include or exclude from the view. To identify the subtree, specify a string using numbers, such as 1.4.2.6.8. Replace a single subidentifier with the asterisk (*) to specify a subtree family.
excluded	Specifies an excluded view.
included	Specifies an included view.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The **snmp-server view** command can include or exclude a group of OIDs. The following example shows how to create a view (named **blockInterfaces**) to exclude the OID subtree family 1.3.3.1.2.1.2:

```
(config)#snmp-server view blockInterfaces 1.3.6.1.2.1.2.* excluded
```

The following example shows how to create a view (named **block**) to include a specific OID:

```
(config)#snmp-server view block 1.3.6.1.2.1.2. included
```

sntp server *<address or hostname>* version *<1-3>*

Use the **sntp server** command to set the hostname of the SNTP server as well as the version of SNTP to use. The Simple Network Time Protocol (SNTP) is an abbreviated version of the Network Time Protocol (NTP). SNTP is used to set the time of the AOS product over a network. The SNTP server usually serves the time to many devices within a network.

Syntax Description

<address or hostname>	Specifies the IP address or hostname of the SNTP server.
version *<1-3>*	Specifies which NTP version is used (1 to 3).

Default Values

By default, NTP version is set to 1.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sets the SNTP server to **time.nist.gov** using SNTP version 1 (the default version):

```
(config)#sntp server time.nist.gov
```

The following example sets the SNTP server as **time.nist.gov**. All requests for time use version 2 of the SNTP:

```
(config)#sntp server time.nist.gov version 2
```

spanning-tree edgeport bpdufilter default

Use the **spanning-tree edgeport bpdufilter default** command to enable the BPDU filter on all ports by default. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

Disabled by default.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The BPDU filter blocks any BPDUs from being transmitted and received on an interface. This can be overridden on an individual port.

Usage Examples

The following example enables the bpdufilter on all ports by default:

```
(config)#spanning-tree edgeport bpdufilter default
```

To disable the BPDU filter on a specific interface, issue the appropriate commands for the given interface using the following commands as an example:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#spanning-tree bpdufilter disable
```

spanning-tree edgeport bpduguard default

Use the **spanning-tree edgeport bpduguard default** command to enable the BPDU guard on all ports by default. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

Disabled by default.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpduguard blocks any BPDUs from being received on an interface. This can be overridden on an individual port.

Usage Examples

The following example enables the BPDU guard on all ports by default.

```
(config)#spanning-tree bpduguard default
```

To disable the BPDU guard on a specific interface, issue the appropriate commands for the given interface using the following commands as an example:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#spanning-tree bpduguard disable
```

spanning-tree edgeport default

Use the **spanning-tree edgeport default** command to configure all ports to be edgeports by default. Use the **no** form of this command to disable the setting.

Syntax Description

No subcommands.

Default Values

Disabled by default.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, and 4000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures all interfaces running spanning tree to be edgeports by default:

```
(config)#spanning-tree edgeport default
```

An individual interface can be configured to not be considered an edgeport. For example:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#spanning-tree edgeport disable
```

or

```
(config)#interface ethernet 0/1
(config-eth 0/1)#no spanning-tree edgeport
```

spanning-tree forward-time *<seconds>*

Use the **spanning-tree forward-time** command to specify the delay interval (in seconds) when forwarding spanning-tree packets. Use the **no** form of this command to return to the default interval.

Syntax Description

<seconds>	Specifies the forwarding delay interval in seconds (Range: 4 to 30).

Default Values

By default, the forwarding delay is set to 15 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the forwarding time to 18 seconds:

```
(config)#spanning-tree forward-time 18
```

spanning-tree hello-time *<seconds>*

Use the **spanning-tree hello-time** command to specify the delay interval (in seconds) between hello bridge protocol data units (BPDUs). To return to the default interval, use the **no** form of this command.

Syntax Description

<seconds>	Specifies the delay interval (in seconds) between hello BPDUs. Range: 0 to 1,000,000.

Default Values

By default, the delay is set to 2 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures a **spanning-tree hello-time** interval of 10,000 seconds:

```
(config)#spanning-tree hello-time 10000
```

spanning-tree max-age *<seconds>*

Use the **spanning-tree max-age** command to specify the interval (in seconds) the spanning tree will wait to receive Bridge Protocol Data Units (BPDUs) from the root bridge before assuming the network has changed (thus re-evaluating the spanning-tree topology). Use the **no** form of this command to return to the default interval.

Syntax Description

<seconds>	Specifies the wait interval (in seconds) between received BPDUs (from the root bridge). Range: 6 to 40.

Default Values

By default, the wait interval is set at 20 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures a wait interval of 45 seconds:

```
(config)#spanning-tree max-age 45
```

spanning-tree mode [rstp | stp]

Use the **spanning-tree mode** command to choose a spanning-tree mode of operation.

Syntax Description

rstp	Enables rapid spanning-tree protocol.
stp	Enables spanning-tree protocol.

Default Values

By default, **spanning-tree mode** is set to **rstp**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the spanning-tree mode to rapid spanning-tree protocol:

```
(config)#spanning-tree mode rstp
```

spanning-tree pathcost method [short | long]

Use the **spanning-tree pathcost** command to select a short or long pathcost method used by the spanning-tree protocol.

Syntax Description

short	Specifies a short pathcost method.
long	Specifies a long pathcost method.

Default Values

By default, **spanning-tree pathcost** is set to **short**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example specifies that the spanning-tree protocol use a long pathcost method:

```
(config)#spanning-tree pathcost method long
```

spanning-tree priority *<value>*

Use the **spanning-tree priority** command to set the priority for spanning-tree interfaces. The lower the priority value, the higher the likelihood the configured spanning-tree interface will be the root for the bridge group. To return to the default bridge priority value, use the **no** version of this command.

Syntax Description

<*value*>	Sets a priority value for the bridge interface. Configuring this value to a low number increases the interface's chance of being the root. Therefore, the maximum priority level would be 0. Range: 0 to 65,535.

Default Values

By default, the priority level is set to 32768.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets **spanning-tree priority** to the maximum level:

```
(config)#spanning-tree priority 0
```

tacacs-server

Use the **tacacs-server** command to customize setting for communication with TACACS servers. Use the **no** form of this command to return to default settings.

Variations of this command include the following:
tacacs-server host *<hostname or IP address>*
tacacs-server host *<hostname or IP address>* **key** *<key>*
tacacs-server host *<hostname or IP address>* **port** *<TCP port>*
tacacs-server host *<hostname or IP address>* **timeout** *<seconds>*
tacacs-server key *<key>*
tacacs-server packet maxsize *<maximum packet size>*
tacacs-server timeout *<seconds>*

Syntax Description<

host *<name/IP>*	Specifies the IP host by name or IP address.
key *<key>*	Sets an encryption string to be used for encrypting and decrypting the traffic between the Network Access Server (NAS) and the TACACS+ daemon. Setting a key for a particular server (using the **tacacs-server host** *<name/IP>* **key** *<key>* command) supersedes keys set globally using the **tacacs-server key** *<key>* command.
port *<tcp port>*	Specifies the TCP port number to be used when connecting to the TACACS+ daemon.
timeout *<seconds>*	Specifies a timeout limit (in seconds) that the unit will wait for a response from the daemon before declaring an error. Range is 1 to 1000 seconds. Setting a timeout for a particular server (using the **tacacs-server host** *<name/IP>* **timeout** *<seconds>* command) supersedes time limits set globally using the **tacacs-server timeout** *<seconds>* command.
packet maxsize *<size>*	Specifies a maximum packet size for this server. Range is 10,240 to 65,535.

Default Values

By default, the key is set to **key** and the default TCP port number is **49**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets a timeout limit of 60 seconds for the specified server:

```
(config)#tacacs-server host 10.5.6.7 timeout 60
```

thresholds [BES | CSS | DM | ES | LCV | LES | PCV | SEFS | SES | UAS] [15Min | 24Hr] *<threshold count>*

Use the **thresholds** command to specify DS1 performance counter thresholds. Use the **no** form of this command to return to default settings.

> *Threshold settings are applied to ALL DS1s.*

Syntax Description

BES	Specifies the bursty errored seconds threshold.
CSS	Specifies the controlled slip seconds threshold.
DM	Specifies the degraded minutes threshold.
ES	Specifies the errored seconds threshold.
LCV	Specifies the line code violations threshold.
LES	Specifies the line errored seconds threshold.
PCV	Specifies the path coding violations threshold.
SEFS	Specifies the severely errored framing seconds threshold.
SES	Specifies the severely errored seconds threshold.
UAS	Specifies the unavailable seconds threshold.
15Min	Specifies that the threshold you are setting is for the counter's 15 minute statistics.
24Hr	Specifies that the threshold you are setting is for the counter's 24 hour statistics.
<threshold>	Specifies the maximum occurrences allowed for this error type. Once a threshold is exceeded, an event is sent to the console specifying the appropriate counter. Additionally, if SNMP traps are enabled, the unit will send a trap with the same information as the console event.

Default Values

The default values for this command are as follows:

thresholds BES 15Min 10
thresholds BES 24Hr 100
thresholds CSS 15Min 1
thresholds CSS 24Hr 4
thresholds DM 15Min 1
thresholds DM 24Hr 4
thresholds ES 15Min 65
thresholds ES 24Hr 648
thresholds LCV 15Min 13340
thresholds LCV 24Hr 133400
thresholds LES 15Min 65
thresholds LES 24Hr 648
thresholds PCV 15Min 72
thresholds PCV 24Hr 691

```
thresholds SES 15Min 10
thresholds SES 24Hr 100
thresholds SEFS 15Min 2
thresholds SEFS 24Hr 17
thresholds UAS 15Min 10
thresholds UAS 24Hr 10
```

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the threshold for the 15 minute and 24 hour bursty errored seconds counter to **25** and **200**, respectively:

```
(config)#thresholds BES 15Min 25
(config)#thresholds BES 24Hr 200
```

username *<username>* **password** *<password>*

Use this command to configure the username and password to use for all protocols requiring a username-based authentication system including FTP server authentication, line (login local-user list), and HTTP access.

Syntax Description

<username>	Specifies a username using an alphanumerical string up to 30 characters in length (the username is case-sensitive).
<password>	Specifies a password using an alphanumerical string up to 30 characters in length (the password is case-sensitive).

Default Values

By default, there is no established username and password.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

All users defined using the **username/password** command are valid for access to the unit using the **login local-userlist** command.

Usage Examples

The following example creates a username of **ADTRAN** with password **ADTRAN**:

```
(config)#username ADTRAN password ADTRAN
```

CODEC List Command Set on page 1586*Voice Trunk Group Command Set* on page 1684*Voice User Command Set* on page 1734*Voice Trunk Analog LS/GS Command Set* on page 1660*Voice Trunk Analog DPT Command Set* on page 1640*Voice Trunk ISDN Command Set* on page 1689*Voice Trunk T1 Wink Command Set* on page 1717*VLAN Configuration Command Set* on page 655

LINE (CONSOLE) INTERFACE CONFIG COMMAND SET

To activate the Line (Console) Interface Configuration mode, enter the **line console 0** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#line console 0
(config-con 0)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

accounting commands [<level> l <name> l default] on page 471

authorization commands [<level> l <name> l default] on page 472

databits [7 | 8] on page 473

flowcontrol [none | software in] on page 474

line-timeout <minutes> on page 475

login on page 476

login authentication <aaa login list> on page 477

login local-userlist on page 478

parity [even | mark | none | odd | space] on page 479

password [md5] <password> on page 480

speed <rate> on page 481

stopbits [1 | 2] on page 482

accounting commands [*<level>* | *<name>* | default]

Use the **accounting commands** command to assign AAA accounting methods to lines. You must first turn AAA on for this command to become available.

Syntax Description

<level>	Specifies a command level (1 or 15).
<name>	Applies a named accounting method to this line.
default	Applies the default accounting method to a line.

Default Values

The default for this command is **off**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example applies the default accounting method to line 1:

```
(config)#aaa on
(config)#line console 0
(config-con0)#accounting commands 1 default
```

authorization commands [<*level*> I <*name*> I default]

Use the **authorization commands** command to assign AAA authorization methods to lines. You must first turn AAA on for this command to become available.

Syntax Description

<*level*>	Specifies a command level (1 or 15).
<*name*>	Applies a named authorization method to this line.
default	Applies the default authorization method to a line.

Default Values

The default for this command is **off**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example applies the default authorization method to line 1:

```
(config)#aaa on
(config)#line console 0
(config-con0)#authorization commands 1 default
```

databits [7 | 8]

Use the **databits** command to set the number of databits per character for a terminal session. This value must match the configuration of your VT100 terminal or terminal emulator software. The default is 8 databits per character. Use the **no** form of this command to return to the default value.

Syntax Description

7	Specifies 7 data bits per character.
8	Specifies 8 data bits per character.

Default Values

By default, the databits are set to 8.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures 7 databits per character for the console terminal session:

```
(config)#line console 0
(config-con 0)#databits 7
```

flowcontrol [none | software in]

Use the **flowcontrol** command to set flow control for the line console.

Syntax Description

none	Specifies no flow control.
software in	Configures AOS to derive flow control from the attached device.

Default Values

By default, flow control is set to none.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example configures no flow control for the line console:

```
(config)#line console 0
(config-con 0)#flowcontrol none
```

line-timeout *<minutes>*

Use the **line-timeout** command to specify the number of minutes a line session may remain inactive before the AOS terminates the session. Use the **no** form of this command to return to the default value.

Syntax Description

<minutes>	Specifies the number of minutes a line session may remain inactive before the AOS terminates the session. Entering a **line-timeout** value of 0 disables the feature.

Default Values

By default the **line-timeout** is set to 15 minutes (Console and Telnet).

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a timeout of 2 minutes:

```
(config)#line console 0
(config-con 0)#line-timeout 2
```

login

Use the **login** command to enable security login on the line session requiring the password configured using the **password** command. Use the **no** form of this command to disable the login feature.

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password on the available console session:

```
(config)#line console 0
(config-console 0)#login
(config-console 0)#password mypassword
```

login authentication *<aaa login list>*

Use the **login authentication** command to specify the named AAA login list to use for authenticating users connecting on this line.

Syntax Description

<aaa login list>	Specifies the AAA login list to use for authentication.

Default Values

The default value is the default AAA list.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

If the AAA subsystem is activated but no login authentication list is given, the default list is used. If the default list is used but the default list is not configured, the behavior for consoles is to be granted access. This prevents a lockout configuration.

Usage Examples

The following example specifies that **myList** will be used for authenticating users connecting on this line:

```
(config)#line console 0
(config-con 0)#login authentication myList
```

login local-userlist

Use the **login local-userlist** command to enable security login for the terminal session requiring the usernames and passwords configured using the **username/password** Global Configuration command. Use the **no** form of this command to disable the login local-userlist feature.

> NOTE *All user properties assigned using the **username/password** command are valid when using the **login local-userlist** command.*

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays creating a local userlist and enabling the security login feature on the **CONSOLE** port:

```
(config)#username my_user password my_password
(config)#line console 0
(config-con 0)#login local-userlist
```

When connecting to the unit, the following prompts are displayed:

```
User Access Login
Username: ADTRAN
Password:
Router#
```

parity [even | mark | none | odd | space]

Use the **parity** command to specify the type of parity used as error correction. This value must match the configuration of your VT100 terminal or terminal emulator software. Use the **no** form of this command to return to the default value.

Syntax Description

even	Sets the parity bit to 0 if the number of 1 bits in the data sequence is odd, or set to 1 if the number of 1 bits is even.
mark	Always sets the parity bit to 1.
none	No parity bit used.
odd	Sets the parity bit to 1 if the number of 1 bits in the data sequence is even, or set to 1 if the number is odd.
space	Always sets the parity bit to 0.

Default Values

By default, the parity option is set to **none**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Parity is the process used to detect whether characters have been altered during the data transmission process. Parity bits are appended to data frames to ensure that parity (whether it be odd or even) is maintained.

Usage Examples

The following example specifies mark parity for the console terminal session:

```
(config)#line console 0
(config-con 0)#parity mark
```

password [md5] *<password>*

Use the **password** command to configure the password (with optional encryption) required on the line session when security login is enabled (using the **login** command). Use the **no** form of this command to remove a configured password.

Syntax Description

md5	Specifies Message Digest 5 (MD5) as the encryption protocol to use when displaying the enable password during show commands. If the MD5 keyword is not used, encryption is not used when displaying the enable password during show commands.
<password>	Specifies the password for the line session using an alphanumeric character string (up to 16 characters).

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 6.1	Added encryption.

Usage Examples

The following example enables the security login feature and specifies a password on the **CONSOLE** port:

```
(config)#line console 0
(config-con 0)#login
(config-con 0)#password mypassword
```

To provide extra security, the AOS can encrypt the enable password when displaying the current configuration. For example, the following is a **show configuration** printout (password portion) with an unencrypted enable password (ADTRAN):

```
!
enable password ADTRAN
!
```

Alternately, the following is a **show configuration** printout (password portion) with an enable password of ADTRAN using md5 encryption:

```
!
enable password md5 encrypted 5aa5fbae7d01a90e79fb57705ce74676
!
```

speed *<rate>*

Use the **speed** command to specify the data rate for the **CONSOLE** port. This setting must match your VT100 terminal emulator or emulator software. Use the **no** form of this command to restore the default value.

Syntax Description

<rate>	Specifies rate of data transfer on the interface (2400; 4800; 9600; 19,200; 38,400; 57,600; or 115,200 bps).

Default Values

By default, the speed is set to 9600 bps.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the **CONSOLE** port for 19200 bps:

```
(config)#line console 0
(config-con 0)#speed 19200
```

stopbits [1 | 2]

Use the **stopbits** command to set the number of stopbits per character for a terminal session. This value must match the configuration of your VT100 terminal or terminal emulator software. The default is 1 stopbit per character. Use the **no** form of this command to return to the default value.

Syntax Description

1	Specifies 1 stopbit per character.
2	Specifies 2 stopbits per character.

Default Values

By default, the **stopbits** are set to **1**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures 2 stopbits per character for the console terminal session:

```
(config)#line console 0
(config-con 0)#stopbits 2
```

LINE (SSH) INTERFACE CONFIG COMMAND SET

To activate the Line Secure Shell (SSH) Interface Configuration mode, enter the **line ssh** command specifying a SSH session(s) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#line ssh 0 4
(config-ssh0-4)#
```

You can select a single line by entering the **line ssh** command followed by the line number (0-4). For example:

```
>enable
#configure terminal
(config)#line ssh 2
(config-ssh2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-class <listname> in on page 484

accounting commands [<level> l <name> l default] on page 485

authorization commands [<level> l <name> l default] on page 486

line-timeout <minutes> on page 487

login on page 488

login authentication <aaa login list> on page 489

login local-userlist on page 490

access-class *<listname>* in

Use the **access-class in** command to restrict Secure Shell (SSH) access using a configured access list. Received packets passed by the access list will be allowed. Use the access list configuration to deny hosts or entire networks or to permit specified IP addresses. See *ip access-list standard <listname> [permit | deny] <ip address>* on page 350 and *ip access-list extended <listname>* on page 344 for more information about configuring access lists.

Syntax Description

<listname>	Identifies the configured access list using an alphanumeric descriptor (all access list descriptors are case-sensitive).

Default Values

By default, there are no configured access lists associated with SH sessions.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

When using the **access-class in** command to associate an access list with an SSH session, remember to duplicate the **access-class in** command for all configured SSH sessions 0 through 4. SSH access to the unit using a particular SSH session is not possible. Users will be assigned the first available SSH session.

Usage Examples

The following example associates the access list **Trusted** (to allow SSH sessions from the 192.22.56.0/24 network) with all SSH sessions (0 through 4):

Create the access list:

```
(config)#ip access-list standard Trusted
(config)#permit 192.22.56.0 0.0.0.255
```

Enter the line (ssh) :

```
(config)#line ssh 0 4
```

Associate the access list with the SSH session:

```
(config-ssh0-4)#access-class Trusted in
```

accounting commands [*<level>* | *<name>* | default]

Use the **accounting commands** command to assign AAA accounting methods to lines. You must first turn AAA on for this command to become available.

Syntax Description

<level>	Specifies a command level (1 or 15).
<name>	Applies a named accounting method to this line.
default	Applies the default accounting method to a line.

Default Values

The default for this command is **off**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example applies the default accounting method to line 1:

```
(config)#aaa on
(config)#line ssh 1
(config-ssh1)#accounting commands 1 default
```

authorization commands [*<level>* | *<name>* | default]

Use the **authorization commands** command to assign AAA authorization methods to lines. You must first turn AAA on for this command to become available.

Syntax Description

<level>	Specifies a command level (1 or 15).
<name>	Applies a named authorization method to this line.
default	Applies the default authorization method to a line.

Default Values

The default for this command is **off**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example applies the default authorization method to line 1:

```
(config)#aaa on
(config)#line ssh 1
(config-ssh1)#authorization commands 1 default
```

line-timeout *<minutes>*

Use the **line-timeout** command to specify the number of minutes a line session may remain inactive before the AOS terminates the session. Use the **no** form of this command to return to the default value.

Syntax Description

<minutes>	Specifies the number of minutes a line session may remain inactive before the AOS terminates the session. Valid range: 0 to 35791. Entering a **line-timeout** value of 0 disables the feature.

Default Values

By default the **line-timeout** is set to 15 minutes.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies a timeout of 2 minutes for all SSH sessions:

```
(config)#line ssh 0 4
(config-ssh0-4)#line-timeout 2
```

login

Use the **login** command to enable security login on the line session requiring the password configured using the **password** command. Use the **no** form of this command to disable the login feature.

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password on all the available SSH sessions (0 through 4):

```
(config)#line ssh 0 4
(config-ssh0-4)#login
(config-ssh0-4)#password mypassword
```

login authentication *<aaa login list>*

Use the **login authentication** command to assign the named AAA login list to use for authenticating users connecting on this line. Use the **no** form of the command to remove the AAA authentication list.

Syntax Description

<aaa login list>	Specifies the name of the AAA login list to use for authentication.

Default Values

The default value is the default AAA list.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

If the AAA subsystem is activated but no login authentication list is given, the default list is used. If the default list is used but the default list is not configured, SSH uses the local user database.

Usage Examples

The following example specifies that **myList** will be used for authenticating users connecting on this line:

```
(config)#line ssh 2
(config-ssh2)#login authentication myList
```

login local-userlist

Use the **login local-userlist** command to check the local list of usernames and passwords configured using the **username/password** Global Configuration command (see *username <username> password <password>* on page 469). Use the **no** form of this command to disable the login local-userlist feature.

> NOTE
>
> *All user properties assigned using the* ***username/password*** *command are valid when using the* ***login local-userlist*** *command.*

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example creates a local userlist and enables the security login feature:

```
(config)#username my_user password my_password
(config)#line ssh 0
(config-ssh0)#login local-userlist
```

When connecting to the unit, the following prompts are displayed:

```
User Access Login
Username: my_user
Password:
#
```

LINE (TELNET) INTERFACE CONFIG COMMAND SET

To activate the Line (Telnet) Interface Configuration mode, enter the **line telnet** command specifying a Telnet session(s) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#line telnet 0 4
(config-telnet0-4)#
```

You can select a single line by entering the **line telnet** command followed by the line number (0-4). For example:

```
>enable
#configure terminal
(config)#line telnet 2
(config-telnet2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-class <listname> in on page 492

accounting commands [<level> l <name> l default] on page 493

authorization commands [<level> l <name> l default] on page 494

line-timeout <minutes> on page 495

login on page 496

login authentication <aaa login list> on page 497

login local-userlist on page 498

password [md5] <password> on page 499

access-class *<listname>* in

Use the **access-class in** command to restrict Telnet access using a configured access list. Received packets passed by the access list will be allowed. Use the access list configuration to deny hosts or entire networks or to permit specified IP addresses. See *ip access-list standard <listname> [permit | deny] <ip address>* on page 350 and *ip access-list extended <listname>* on page 344 for more information about configuring access lists.

Syntax Description

<listname>	Identifies the configured access list using an alphanumeric descriptor (all access list descriptors are case-sensitive).

Default Values

By default, there are no configured access lists associated with Telnet sessions.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

When using the **access-class in** command to associate an access list with a Telnet session, remember to duplicate the **access-class in** command for all configured Telnet sessions 0 through 4. Telnet access to the unit using a particular Telnet session is not possible. Users will be assigned the first available Telnet session.

Usage Examples

The following example associates the access list **Trusted** (to allow Telnet sessions from the 192.22.56.0/24 network) with all Telnet sessions (0 through 4):

Create the access list:

```
(config)#ip access-list standard Trusted
(config)#permit 192.22.56.0 0.0.0.255
```

Enter the line (telnet):

```
(config)#line telnet 0 4
```

Associate the access list with the Telnet session:

```
(config-telnet0-4)#access-class Trusted in
```

accounting commands [<*level*> | <*name*> | default]

Use the **accounting commands** command to assign AAA accounting methods to lines. You must first turn AAA on for this command to become available.

Syntax Description

<*level*>	Specifies a command level (1 or 15).
<*name*>	Applies a named accounting method to this line.
default	Applies the default accounting method to a line.

Default Values

The default for this command is **off**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example applies the default accounting method to Telnet session 1:

```
(config)#aaa on
(config)#line telnet 1
(config-telnet1)#accounting commands 1 default
```

authorization commands [*<level>* | *<name>* | default]

Use the **authorization commands** command to assign AAA authorization methods to lines. You must first turn AAA on for this command to become available.

Syntax Description

<level>	Specifies a command level (1 or 15).
<name>	Applies a named authorization method to this line.
default	Applies the default authorization method to a line.

Default Values

The default for this command is **off**.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example applies the default authorization method to line 1:

```
(config)#aaa on
(config)#line telnet 1
(config-telnet1)#authorization commands 1 default
```

line-timeout *<minutes>*

Use the **line-timeout** command to specify the number of minutes a line session may remain inactive before the AOS terminates the session. Use the **no** form of this command to return to the default value.

Syntax Description

<minutes>	Specifies the number of minutes a line session may remain inactive before the AOS terminates the session. Entering a **line-timeout** value of 0 disables the feature.

Default Values

By default the **line-timeout** is set to 15 minutes (Console and Telnet).

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a timeout of 2 minutes:

```
(config)#line telnet 0
(config-telnet0)#line-timeout 2
```

login

Use the **login** command to enable security login on the line session requiring the password configured using the **password** command. Use the **no** form of this command to disable the login feature.

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password on all the available Telnet sessions (0 through 4):

```
(config)#line telnet 0 4
(config-telnet0-4)#login
(config-telnet0-4)#password mypassword
```

login authentication *<aaa login list>*

Use the **login authentication** command to specify the named AAA login list to use for authenticating users connecting on this line.

Syntax Description

<aaa login list>	Specifies the AAA login list to use for authentication.

Default Values

The default value is the default AAA list.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

If the AAA subsystem is activated but no login authentication list is given, the default list is used. If the default list is used but the default list is not configured, the behavior for telnets is to use the local user database.

Usage Examples

The following example specifies that **myList** will be used for authenticating users connecting on this line:

```
(config)#line telnet 2
(config-telnet2)#login authentication myList
```

login local-userlist

Use the **login local-userlist** command to enable security login for the terminal session requiring the usernames and passwords configured using the **username/password** Global Configuration command. Use the **no** form of this command to disable the login local-userlist feature.

> NOTE *All user properties assigned using the **username/password** command are valid when using the **login local-userlist** command.*

Syntax Description

No subcommands.

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example displays creating a local userlist and enabling the security login feature:

```
(config)#username my_user password my_password
(config)#line telnet 0
(config-telnet0)#login local-userlist
```

When connecting to the unit, the following prompts are displayed:

```
User Access Login
Username: my_user
Password:
Router#
```

password [md5] *<password>*

Use the **password** command to configure the password (with optional encryption) required on the line session when security login is enabled (using the **login** command). Use the **no** form of this command to remove a configured password.

Syntax Description

md5	Optional. Specifies Message Digest 5 (MD5) as the encryption protocol to use when displaying the enable password during show commands. If the MD5 keyword is not used, encryption is not used when displaying the enable password during show commands.
<password>	Specifies the password for the line session using an alphanumeric character string (up to 16 characters).

Default Values

By default, there is no login password set for access to the unit.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and
Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables the security login feature and specifies a password for the Telnet session 0:

```
(config)#line telnet 0
(config-telnet0)#login
(config-telnet0)#password mypassword
```

To provide extra security, the AOS can encrypt the enable password when displaying the current configuration. For example, the following is a **show configuration** printout (password portion) with an unencrypted enable password (ADTRAN):

```
!
enable password ADTRAN
!
```

Alternately, the following is a **show configuration** printout (password portion) with an enable password of ADTRAN using md5 encryption:

```
!
enable password md5 encrypted 5aa5fbae7d01a90e79fb57705ce74676
```

DSX-1 INTERFACE CONFIGURATION COMMAND SET

To activate the DSX-1 Interface Configuration mode, enter the **interface t1** command (and specify the DSX-1 port) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface t1 1/2
(config-t1 1/2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

coding [ami | b8zs] on page 501

framing [d4 | esf] on page 502

line-length <value> on page 503

loopback network [line | payload] on page 504

loopback remote line [inband] on page 505

remote-loopback on page 506

signaling-mode [message-oriented | none | robbed-bit] on page 507

snmp trap link-status on page 508

test-pattern [ones | zeros] on page 509

coding [ami | b8zs]

Use the **coding** command to configure the line coding for a DSX-1 physical interface. This setting must match the line coding supplied on the circuit by the PBX.

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
b8zs	Configures the line coding for bipolar eight zero substitution (B8ZS).

Default Values

By default, all DSX-1 interfaces are configured with B8ZS line coding.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the DSX-1 circuit. A mismatch will result in line errors (e.g., BPVs).

Usage Examples

The following example configures the DSX-1 interface for AMI line coding:

```
(config)#interface t1 1/2
(config-t1 1/2)#coding ami
```

framing [d4 | esf]

Use the **framing** command to configure the framing format for the DSX-1 interface. This parameter should match the framing format set on the external device. Use the **no** form of this command to return to the default value.

Syntax Description

d4	Specifies D4 superframe (SF) format.
esf	Specifies extended superframe (ESF) format.

Default Values

By default, the framing format is set to **esf**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

A frame is comprised of a single byte from each of the T1’s timeslots; there are 24 timeslots on a single T1 circuit. Framing bits are used to separate the frames and indicate the order of information arriving at the receiving equipment. D4 and ESF are two methods of collecting and organizing frames over the circuit.

Usage Examples

The following example configures the DSX-1 interface for D4 framing:

```
(config)#interface t1 1/2
(config-t1 1/2)#framing d4
```

line-length *<value>*

Use the **line-length** command to set the line build out (in feet or dB) for the DSX-1 interface. Use the **no** form of this command to return to the default value.

Syntax Description

<value>	Configures the line build out for the DSX-1 interface. Valid options include: -7.5 dB or 0 to 655 feet. Use the -7.5 dB option for maximum attenuation.

Default Values

By default, the line build out is set to 0 feet.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **line-length** value represents the physical distance between DSX equipment (measured in cable length). Based on this setting, the AOS device increases signal strength to compensate for the distance the signal must travel. Valid distance ranges are listed below:

- 0 to 133 feet
- 134 to 265 feet
- 266 to 399 feet
- 400 to 533 feet
- 534 to 655 feet

Usage Examples

The following example configures the DSX-1 interface **line-length** for 300 feet:

```
(config)#interface t1 1/2
(config-t1 1/2)#line-length 300
```

loopback network [line | payload]

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback.

Syntax Description

line	Initiates a metallic loopback of the physical DSX-1 network interface.
payload	Initiates a loopback of the T1 framer (CSU portion) of the DSX-1 network interface.

Default Values

No default necessary for this command.

Applicable Platforms

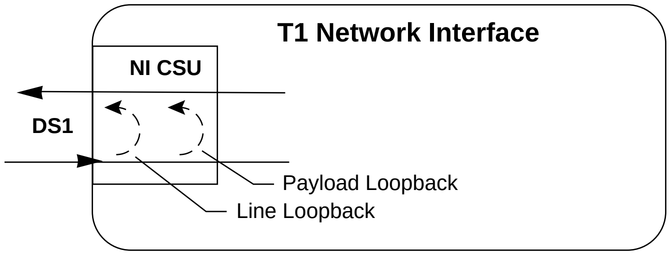
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a payload loopback of the DSX-1 interface:

```
(config)#interface t1 1/2
(config-t1 1/2)#loopback network payload
```

loopback remote line [inband]

Use the **loopback remote line inband** command to send a loopback code to the remote unit to initiate a line loopback. Use the **no** form of this command to send a loopdown code to the remote unit to deactivate the loopback.

Syntax Description

inband	Uses the inband channel to initiate a full 1.544 Mbps physical (metallic) loopback of the signal received by the remote unit from the network.

Default Values

No defaults necessary for this command.

Applicable Platforms

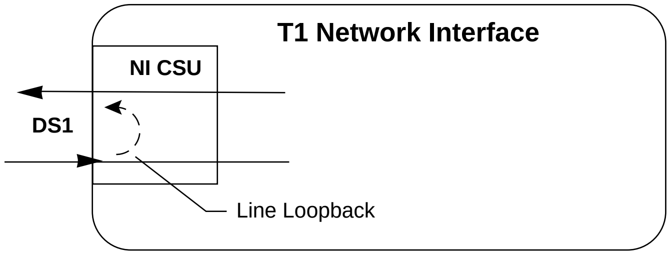
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

A remote loopback can only be issued if a cross-connect does not exist on the interface and if the signaling mode is set to **none**. The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a remote line loopback using the inband channel:

```
(config)#interface t1 1/2
(config-t1 1/2)#loopback remote line inband
```

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables remote loopbacks on the DSX-1 interface:

```
(config)#interface t1 1/2
(config-t1 1/2)#remote-loopback
```

signaling-mode [message-oriented | none | robbed-bit]

Use the **signaling-mode** command to configure the signaling type (robbed-bit for voice or clear channel for data) for the DS0s mapped to the DSX-1 port.

Syntax Description

message-oriented	Specifies clear channel signaling on Channel 24 only. Use this signaling type with QSIG installations.
none	Specifies clear channel signaling on all 24 DS0s. Use this signaling type with data-only or PRI DSX-1 installations.
robbed-bit	Specifies robbed bit signaling on all DS0s. Use this signaling type for voice-only DSX-1 applications.

Default Values

By default, the signaling mode is set to robbed-bit.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the DSX-1 port for PRI compatibility:

```
(config)#interface t1 1/2
(config-t1 1/2)#signaling-mode none
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit-Ethernet, port-channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the DSX-1 interface:

```
(config)#interface t1 1/2
(config-t1 1/2)#no snmp trap link-status
```

test-pattern [ones | zeros]

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation.

Syntax Description

ones	Generates a test pattern of continous ones.
zeros	Generates a test pattern of continous zeros.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example activates the pattern generator for a stream of continuous ones:

```
(config)#interface t1 1/2
(config-t1 1/2)#test-pattern ones
```

E1 Interface Configuration Command Set

To activate the E1 Interface Configuration mode, enter the **interface e1** command (and specify the E1 port) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface e1 1/1
(config-e1 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

clock source [internal | line | through] on page 511

coding [ami | hdb3] on page 512

framing [crc4] on page 513

loop-alarm-detect on page 514

loopback network [line | payload] on page 515

loopback remote v54 on page 516

remote-alarm [rai | ais] on page 517

remote-loopback on page 518

sa4tx-bit [0 | 1] on page 519

show test-pattern on page 520

snmp trap line-status on page 521

snmp trap link-status on page 522

snmp trap threshold-reached on page 523

tdm-group <group number> timeslots <1-31> speed [56 | 64] on page 524

test-pattern [clear | insert | ones| p215 | p220 | p511 | qrss | zeros] on page 525

ts16 on page 526

clock source [internal | line | through]

Use the **clock source** command to configure the source timing used for the interface. Use the **no** form of this command to return to the default value.

Syntax Description

internal	Configures the unit to provide clocking using the internal oscillator.
line	Configures the unit to recover clocking from the E1 circuit.
through	Configures the unit to recover clocking from the circuit connected to the G.703 interface.

Default Values

By default, the unit is configured to recover clocking from the primary circuit.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

When operating on a circuit that is providing timing, setting the **clock source** to **line** can avoid errors such as Clock Slip Seconds (CSS).

Usage Examples

The following example configures the unit to recover clocking from the primary circuit:

```
(config)#interface e1 1/1
(config-e1 1/1)#clock source line
```

coding [ami | hdb3]

Use the **coding** command to configure the line coding for the E1 physical interface. This setting must match the line coding supplied on the circuit by the service provider.

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
hdb3	Configures the line coding for high-density bipolar 3 (HDB3).

Default Values

By default, all E1 interfaces are configured with HDB3 line coding.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the E1 circuit. A mismatch will result in line errors (e.g., BPVs).

Usage Examples

The following example configures the E1 interface for AMI line coding:

```
(config)#interface e1 1/1
(config-e1 1/1)#coding ami
```

framing [crc4]

Use the **framing** command to configure the framing format for the E1 interface. This parameter should match the framing format provided by the service provider or external device. Use the **no** form of this command to return to the default value.

Syntax Description

crc4	Enables CRC-4 bits to be transmitted in the outgoing data stream. Also, the received signal is checked for CRC-4 errors.

Default Values

By default, CRC-4 is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The framing value must match the configuration of the E1 circuit. A mismatch will result in a loss of frame alarm.

Usage Examples

The following example configures the E1 interface for CRC-4 framing:

```
(config)#interface e1 1/1
(config-e1 1/1)#framing crc4
```

loop-alarm-detect

The **loop-alarm-detect** command enables detection of a loop alarm on the E1 interface. Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command enables the detection of a loopback alarm. This alarm works in conjunction with the **sa4tx-bit** command setting. The loopback condition is detected by comparing the transmitted **sa4tx-bit** value to the received Sa4 bit value. If the bits match, a loopback is assumed. This detection method only works with a network in which the far end is transmitting the opposite value for Sa4.

Usage Examples

The following example enables detection of a loop alarm on the E1 interface:

```
(config)#config e1 1/1
(config-e1 1/1)#loop-alarm-detect
```

loopback network [line | payload]

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback.

Syntax Description

line	Initiates a metallic loopback of the physical E1 network interface.
payload	Initiates a loopback of the E1 framer (CSU) portion of the E1 network interface.

Default Values

No default necessary for this command.

Applicable Platforms

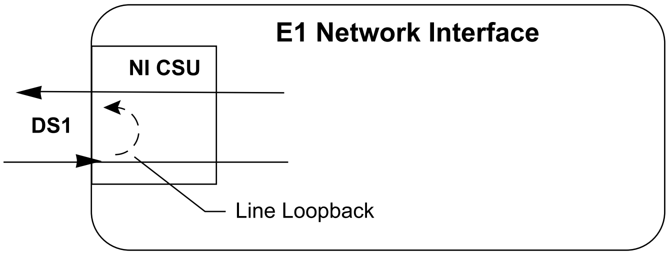
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The following diagram depicts a line loopback.



Usage Examples

The following example initiates a line loopback of the E1 interface:

```
(config)#interface e1 1/1
(config-e1 1/1)#loopback network line
```

loopback remote v54

The **loopback remote v54** command initiates an E1 remote loopback test (with a V.54 loopback pattern). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

This command causes a V.54 inband loop code to be sent in the payload towards the far end.

Usage Examples

The following example sends a V.54 inband loop code to the far end:

```
(config)#interface e1 1/1
(config-e1 1/1)#loopback remote v54
```

remote-alarm [rai | ais]

The **remote-alarm** command selects the alarm signaling type to be sent when a loss of frame is detected on the E1 receive signal. Use the **no** form of this command to disable all transmitted alarms.

Syntax Description

rai	Specifies sending a remote alarm indication (RAI) in response to a loss of frame. Also prevents a received RAI from causing a change in interface operational status.
ais	Sends an alarm indication signal (AIS) as an unframed all-ones signal.

Default Values

The default for this command is **rai**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

An E1 will respond to a loss of frame on the receive signal by transmitting a remote alarm to the far end to indicate the error condition. TS0 of an E1 contains the Frame Alignment Signal (FAS) in the even-numbered frames. The odd-numbered frames are not used for frame alignment, and some of those bits are labeled as spare bits (Sa bits) in bit positions 4 through 8.

Usage Examples

The following example enables transmission of AIS in response to a loss of frame:

```
config)#interface e1 1/1
(config-e1 1/1)#remote alarm ais
```

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

This controls the acceptance of any remote loopback requests. When enabled, remote loopbacks are detected and cause a loopback to be applied. When disabled, remote loopbacks are ignored.

Usage Examples

The following example enables remote loopbacks on the E1 interface:

```
(config)#interface e1 1/1
(config-e1 1/1)#remote-loopback
```

sa4tx-bit [0 | 1]

The **sa4tx-bit** command selects the Tx value of Sa4 in this E1 interface. Use the **no** form of this command to return to the default value of 1.

Syntax Description

No subcommands.

Default Values

The default value for this command is 1.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 6.1 Command was introduced.

Functional Notes

This command assigns a value to the Tx spare bit in position 4. The odd-numbered frames of TS0 are not used for frame alignment. Bits in position 4 through 8 are called spare bits. Values of 0 or 1 are accepted.

TS0 odd frame

Bit position	1	2	3	4	5	6	7	8
Bit use	0	1	RAI = 1	S	S	S	S	S

Usage Examples

The following example sets the Tx value of Sa4 to 0:

```
(config)#interface e1 1/1
(config-e1 1/1)#sa4tx-bit 0
```

show test-pattern

Use the **show test-pattern** command to display results from test patterns inserted using the **test-pattern** command (see *test-pattern [clear | insert | ones| p215 | p220 | p511 | qrss | zeros]* on page 525 for more information).

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following is sample output from this command:

```
(config)#interface e1 1/1
(config-e1 1/1)#show test-pattern
QRSS Errored Seconds: 6
```

snmp trap line-status

Use the **snmp trap line-status** command to control the Simple Network Management Protocol (SNMP) variable dsx1LineStatusChangeTrapEnable (RFC2495) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the dsx1LineStatusChangeTrapEnable OID is set to enabled for all interfaces except virtual Frame Relay Interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 units.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **snmp trap line-status** command is used to control the RFC2495 dsx1LineStatusChangeTrapEnable OID (OID number 1.3.6.1.2.1.10.18.6.1.17.0).

Usage Examples

The following example disables the line-status trap on the T1 interface:

```
(config)#interface e1 1/1
(config-t1 1/1)#no snmp trap line-status
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the E1 interface:

```
(config)#interface e1 1/1
(config-e1 1/1)#no snmp trap link-status
```

snmp trap threshold-reached

Use the **snmp trap threshold-reached** command to control the Simple Network Management Protocol (SNMP) variable adGenAOSDs1ThresholdReached (adGenAOSDs1-Ext MIB) to enable the interface to send SNMP traps when a DS1 performance counter threshold is reached. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the adGenAOSDs1ThresholdReached OID is enabled for all interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables SNMP threshold reached trap on the E1 interface:

```
(config)#interface e1 1/1
(config-e1 1/1)#no snmp trap threshold-reached
```

tdm-group *<group number>* timeslots *<1-31>* speed [56 | 64]

Use the **tdm-group** command to create a group of contiguous channels on this interface to be used during the **cross-connect** process. See *crypto map <mapname>* on page 896 for related information.

> CAUTION
>
> *Changing **tdm-group** settings could result in service interruption.*

Syntax Description

<group number>	Identifies the created TDM group (valid range: 1 to 255).
timeslots *<1-31>*	Specifies the channels to be used in the TDM group. This can be entered as a single number representing one of the 31 E1 channel timeslots or as a contiguous group of channels. (For example, **1-10** specifies the first 10 channels of the E1.)
speed [56 | 64]	Optional. Specifies the individual channel rate on the E1 interface to be 56 kbps or 64 kbps. The default speed is 64 kbps.

Default Values

By default, there are no configured TDM groups.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example creates a TDM group (labeled **5**) of 10 DS0s at 64 kbps each:

```
(config)#interface e1 1/1
(config-e1 1/1)#tdm-group 5 timeslots 1-10 speed 64
```

test-pattern [clear | insert | ones| p215 | p220 | p511 | qrss | zeros]

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation.

Syntax Description

clear	Clears the test pattern error count.
insert	Inserts an error into the currently active test pattern. Display the injected error result using the **show test-pattern** command.
ones	Generates test pattern of continous ones.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.
p220	Generates a pseudorandom test pattern sequence based on a 20-bit shift register.
p511	Generates a test pattern of repeating ones and zeros.
qrss	Generates a test pattern of random ones and zeros.
zeros	Generates test pattern of continous zeros.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example activates the pattern generator for a stream of continuous ones:

```
(config)#interface e1 1/1
(config-e1 1/1)#test-pattern ones
```

ts16

Use the **ts16** command to enable timeslot 16 multiframe to be checked on the receive signal. Use the **no** form of this command to disable timeslot 16.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables timeslot 16 multiframing:

```
(config)#interface e1 1/1
(config-e1 1/1)#ts16
```

ETHERNET INTERFACE CONFIGURATION COMMAND SET

There are four types of Ethernet interfaces associated with the AOS:

- Basic Ethernet interfaces (e.g., eth 0/1)
- Gigabit Ethernet interfaces (e.g., giga-eth 0/3)
- Ethernet sub-interfaces associated with a VLAN (e.g., eth 0/1.1)
- Ethernet interface range (e.g., eth 0/1, 0/8)

To activate the basic Ethernet Interface Configuration mode, enter the **interface ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ethernet 0/1
(config-eth 0/1)#
```

To activate the Gigabit Ethernet Interface Configuration mode, enter the **interface gigabit-ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface gigabit-ethernet 0/3
(config-giga-eth 0/3)#
```

To activate the Ethernet Sub-Interface Configuration mode, enter the **interface ethernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ethernet 0/1.1
(config-eth 0/1.1)#
```

To activate the Ethernet Configuration mode for a range of Ethernet interfaces, enter the **interface range** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface range ethernet 0/1, 0/8
(config-eth 0/1, 0/8)#
```

NOTE *Not all Ethernet commands apply to all Ethernet types. Use the ? command to display a list of valid commands. For example:*

```
>enable
Password:xxxxx
#config term
(config)#int eth 0/1
(config-eth 0/1)#?
access-policy     - Assign access control policy for this interface
alias             - A text name assigned by an SNMP NMS
arp               - Set ARP commands
bandwidth         - Set bandwidth informational parameter
bridge-group      - Assign the current interface to a bridge group
etc....
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 530

arp arpa on page 533

bandwidth <value> on page 534

bridge-group <group#> on page 535

crypto map <mapname> on page 536

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 538

encapsulation 802.1q on page 540

full-duplex on page 541

half-duplex on page 543

ip commands begin on page 544

lldp receive on page 573

lldp send [management-address l port-description l system-capabilities l system-description l system-name l and-receive] on page 574

mac-address <address> on page 576

mtu <size> on page 578

qos-policy out <mapname> on page 579

snmp trap on page 581

snmp trap link-status on page 582

spanning-tree commands begin on page 583

speed [10 | 100 | auto | nonegotiate] on page 589

vlan-id <vlan id> [native] on page 591

vlan-id <vlan id> [native] on page 591

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic to an interface. Use the **no** form of this command to remove an access policy association.

> *Configured access policies will only be active if the* ***ip firewall*** *command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<policyname>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.
Release 6.1	Command was expanded to include VLAN interfaces.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** *<policy name>*.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the Ethernet 0/1 interface:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:
(config)#**ip policy-class UnTrusted**
(config-policy-class)#**allow list InWeb**

Associate the access policy with the Ethernet 0/1 interface:
(config)#**interface ethernet 0/1**
(config-eth 0/1)#**access-policy UnTrusted**

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of the AOS using the **ip firewall** command.

Step 2:
Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a "range." Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a "don't care." For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:
Create an IP policy class that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (access list) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>
All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>
All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>
All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the Ethernet 0/1 interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#access-policy MatchAll
```

arp arpa

Use the **arp arpa** command to enable address resolution protocol (ARP) on the Ethernet interface.

Syntax Description

arpa	Sets standard address resolution protocol for this interface.

Default Values

The default for this command is arpa.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces and Gigabit Ethernet interfaces.

Usage Examples

The following example enables standard ARP for the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#arp arpa
```

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies bandwidth in kbps.

Default Values

To view default values, use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the Ethernet 0/1 interface to 10 Mbps:

```
(config)#interface eth 0/1
(config-eth 0/1)#bandwidth 10000
```

bridge-group *<group#>*

Use the **bridge-group** command to assign an interface to the specified bridge group. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<group#>	Specifies the bridge group number (1 to 255).

Default Values

By default, there are no configured bridge groups.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (e.g., Ethernet to T1 bridge, Ethernet to Frame Relay sub-interface).

Usage Examples

The following example assigns the Ethernet interface to bridge-group 17:

```
(config)#interface eth 0/1
(config-eth 0/1)#bridge-group 17
```

crypto map <*mapname*>

Use the **crypto map** command to associate crypto maps with the interface.

> *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

<*mapname*>	Specifies the crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

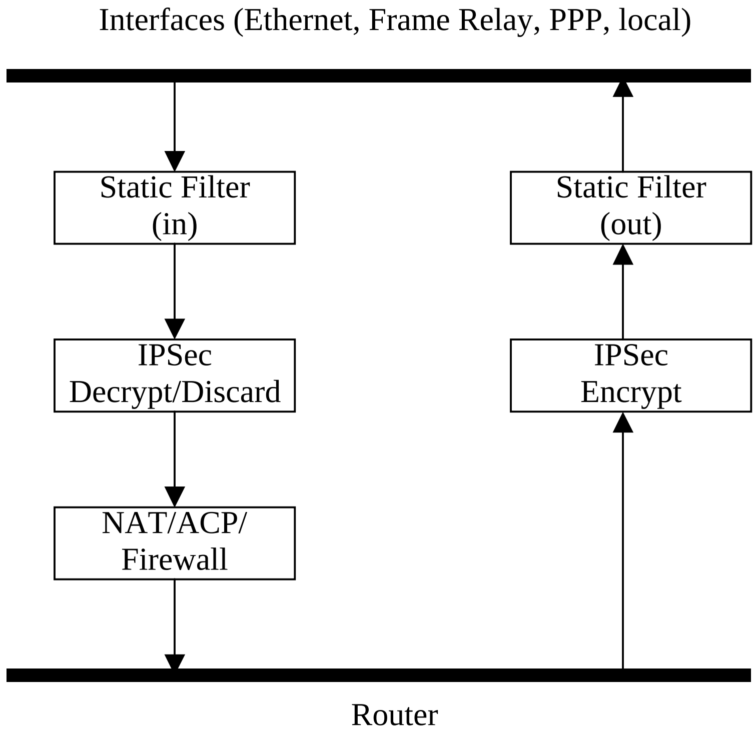
Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following notes in mind.

When defining the policy class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#crypto map MyMap
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

Refer to *Functional Notes* below for argument descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address does not change often or at all but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the dynamic-dns to **dyndns-custom** with hostname **host**, username **user**, and password **pass**:

```
(config)#interface eth 0/1
(config-eth 0/1)#dynamic-dns dyndns-custom host user pass
```

encapsulation 802.1q

Use the **encapsulation 802.1q** command to put the interface into 802.1q (VLAN) mode.

Syntax Description

No subcommands.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example puts interface **eth 0/1** in 802.1q mode and configures a sub-interface for VLAN usage:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#encapsulation 802.1q
(config-eth 0/1)#interface ethernet 0/1.1
(config-eth 0/1.1)vlan-id 3
```

full-duplex

Use the **full-duplex** command to configure the Ethernet interface for full-duplex operation. This allows the interface to send and receive simultaneously. Use the **no** form of this command to return to the default **half-duplex** operation.

Syntax Description

No subcommands.

Default Values

By default, all Ethernet interfaces are configured for half-duplex operation.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000
and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Full-duplex Ethernet is a variety of Ethernet technology currently being standardized by the IEEE. Because there is no official standard, vendors are free to implement their independent versions of full-duplex operation. Therefore, it is not safe to assume that one vendor's equipment will work with another.

Devices at each end of a full-duplex link have the ability to send and receive data simultaneously over the link. Theoretically, this simultaneous action can provide twice the bandwidth of normal (half-duplex) Ethernet. To deploy full-duplex Ethernet, each end of the link must only connect to a single device (a workstation or a switched hub port). With only two devices on a full-duplex link, there is no need to use the medium access control mechanism (to share the signal channel with multiple stations) and listen for other transmissions or collisions before sending data.

> NOTE *If the **speed** is manually set to **10** or **100,** the duplex must be manually configured as **full-duplex** or **half-duplex**. Refer to speed [10 | 100 | auto | nonegotiate]* on page 589 *for more information.*

The 10BaseT, 100BaseTX, and 100BaseFX signalling systems support full-duplex operation (because they have transmit and receive signal paths that can be simultaneously active).

Usage Examples

The following example configures the Ethernet interface for **full-duplex** operation:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#full-duplex
```

half-duplex

Use the **half-duplex** command to configure the Ethernet interface for half-duplex operation. This setting allows the Ethernet interface to either send or receive at any given moment, but not simultaneously. Use the **no** form of this command to disable half-duplex operation.

Syntax Description

No subcommands.

Default Values

By default, all Ethernet interfaces are configured for half-duplex operation.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000
and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Half-duplex Ethernet is the traditional form of Ethernet that employs the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) protocol to allow two or more hosts to share a common transmission medium while providing mechanisms to avoid collisions. A host on a half-duplex link must “listen” on the link and only transmit when there is an idle period. Packets transmitted on the link are broadcast (so it will be “heard” by all hosts on the network). In the event of a collision (two hosts transmitting at once), a message is sent to inform all hosts of the collision and a backoff algorithm is implemented. The backoff algorithm requires the station to remain silent for a random period of time before attempting another transmission. This sequence is repeated until a successful data transmission occurs.

NOTE

*If the **speed** is manually set to **10** or **100,** the duplex must be manually configured as **full-duplex** or **half-duplex**. Refer to speed [10 | 100 | auto | nonegotiate] on page 589 for more information.*

Usage Examples

The following example configures the Ethernet interface for **half-duplex** operation:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#half-duplex
```

ip access-group *<listname>* [in | out]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Assigns IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic (as defined in the user-configured **TelnetOnly** IP access list) into the Ethernet interface:

```
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#interface eth 0/1
(config-eth 0/1)#ip access-group TelnetOnly in
```

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the Ethernet interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface.

ip address dhcp [client-id [<*interface*> | <*identifier*>] hostname <*"string"*>]

Syntax Description

client-id
Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.

<*interface*>
Specifying an interface defines the client identifier as the hexadecimal MAC address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type).

For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address <hardware-address> <type>* on page 1152 for a detailed listing of media types.

<*identifier*>
Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters).

For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the <*identifier*> option.

hostname
Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field.

<*"string"*>
String (encased in quotation marks) of up to 35 characters to use as the name of the host for DHCP operation.

no-default-route
Keyword used to specify that the AOS not install the default-route obtained via DHCP.

no-domain-name
Keyword used to specify that the AOS not install the domain-name obtained via DHCP.

no-nameservers
Keyword used to specify that the AOS not install the DNS servers obtained via DHCP.

Default Values

client-id
Optional. By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address <hardware-address> <type>* on page 1152 for a detailed listing of media types) and the MAC ADDRESS is the Media Access Control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet interface 0/1 is used in this field).

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:

8	7	6	5	4	3	2	1
DLCI (high order)						C/R	EA
DLCI (lower)				FECN	BECN	DE	EA

Where the FECN, BECN, C/R, DE, and high order EA bits are assumed to be 0 and the lower order extended address (EA) bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:
DLCI (decimal) / Q.922 address (hex):

16 / 0x0401

50 / 0x0C21

60 / 0x0CC1

70 / 0x1061

80 / 0x1401

hostname Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field.

<"string"> By default, the hostname is the name configured using the Global Configuration **hostname** command.

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1 Command was introduced.

Functional Notes

Dynamic Host Configuration Protocol (DHCP) allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many Internet Service Providers (ISPs) require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **host-name** fields.

Usage Examples

The following example enables DHCP operation on Ethernet interface 0/1:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip address dhcp
```

ip address *<address>* *<mask>* secondary

Use the **ip address** command to define an IP address on the specified interface (only one primary address is allowed). Use the optional **secondary** keyword to define a secondary IP address. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<*address*>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<*mask*>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Keyword used to configure secondary IP addresses for the specified interface. Multiple secondary IP addresses may be assigned (no limit).

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

Use secondary IP addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IP addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IP addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IP address of **192.22.72.101/30**:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ip address 192.22.72.101 255.255.255.252 secondary
```

ip dhcp release

Use the **ip dhcp release** command to transmit a message to the DHCP server requesting termination of the IP address lease on that interface.

> CAUTION *If you are currently connected to the unit using a Telnet session through the Ethernet interface, using the* ***ip dhcp release*** *command will terminate your Telnet session and render your Telnet capability inoperable until a new IP address is assigned by the DHCP server.*

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Dynamic Host Configuration Protocol (DHCP) allows interfaces to acquire a dynamically-assigned IP address from a configured DHCP server on the network. Many Internet Service Providers (ISPs) require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain.

Usage Examples

The following example releases the IP address assigned (by DHCP) on the Ethernet interface (**eth 0/1**):

```
(config)#int eth 0/1
(config-eth 0/1)#ip dhcp release
```

ip dhcp renew

Use the **ip dhcp renew** command to transmit a message to the DHCP server requesting renewal of the IP address lease on that interface.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Dynamic Host Configuration Protocol (DHCP) allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many Internet Service Providers (ISPs) require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain.

Usage Examples

The following example renews the IP address assigned (by DHCP) on the Ethernet interface (**eth 0/1**):

```
(config)#int eth 0/1
(config-eth 0/1)#ip dhcp renew
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The* ***ip helper-address*** *command must be used in conjunction with the* ***ip forward-protocol*** *command to configure the AOS to forward UDP broadcast packets.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

```
(config)#ip forward-protocol udp domain
(config)#interface eth 0/1
(config-eth 0/1)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description

immediate-leave	If only one host (or IGMP snooping switch) is connected to the interface when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval <*milliseconds*>	This command controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer (if no receiver responds) the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65,535 ms. Default: 1000 ms.
querier-timeout <*seconds*>	Number of seconds that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range: 60 to 300 seconds. Default: 2x the **query-interval** value.
query-interval <*seconds* >	Interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65,535 seconds. Default: 60 seconds.
query-max-response-time <*seconds*>	Maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group <*group-address*>	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface's IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 300, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface, and to place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub upstream* on page 557 for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip mcast-stub downstream
```

ip mcast-stub helper-address *<ip address>*

Use the **ip mcast-stub helper-address** command to specify an IP address toward which IGMP host reports and leave messages are forwarded. This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub downstream** and **ip mcast-stub upstream** commands. Use the **no** form of this command to return to default.

Syntax Description

<*ip address*>	Specifies the address to which the IGMP host reports and leave messages are forwarded.

Default Values

By default, no helper-address is configured.

Applicable Platforms

This command applies to the NetVanta 300, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

The helper address is configured globally and applies to all multicast-stub downstream interfaces. The address specified may be the next upstream hop or any upstream address on the distribution tree for the multicast source, up to and including the multicast source. The router selects, from the list of multicast-stub upstream interfaces, the interface on the shortest path to the specified address. The router then proxies, on the selected upstream interface (using an IGMP host function), any host joins/leaves received on the downstream interface(s). The router retransmits these reports with addresses set as if the report originated from the selected upstream interface.

For example, if the router receives multiple joins for a group, it will not send any extra joins out the upstream interface. Also, if it receives a leave, it will not send a leave until it is certain that there are no more subscribers on any downstream interface.

Usage Examples

The following example specifies 172.45.6.99 as the helper address:

```
(config)#ip mcast-stub helper-address 172.45.6.99
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub downstream* on page 555 for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key *<password>*	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost *<value>*	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 1 to 65,535.
dead-interval *<seconds>*	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, the neighboring device is assumed to be down. Range: 0 to 32,767.
hello-interval *<seconds>*	Specifies the interval between hello packets sent on the interface. Range: 0 to 32,767.
message-digest-key *<keyid>* **md5** *<key>*	Configures OSPF Message Digest 5 (MD5) authentication (16-byte max) keys.
priority *<value>*	Sets the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0 to 255.
retransmit-interval *<seconds>*	Specifies the time between link-state advertisements (LSAs). Range: 0 to 32,767.
transmit-delay *<seconds>*	Sets the estimated time required to send an LSA on the interface. Range: 0 to 32,767.

Default Values

dead-interval *<seconds>*	40 seconds
hello-interval *<seconds>*	10 seconds: Ethernet, point-to-point, Frame Relay, and PPP
retransmit-interval *<seconds>*	5 seconds
transmit-delay *<seconds>*	1 second

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Selects message-digest authentication type.
null	Optional. Specifies that no authentication is used.

Default Values

By default, this is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Usage Examples

The following example specifies that no authentication will be used on the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP and Frame Relay default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip ospf network broadcast
```

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM Sparse Mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip pim sparse-mode
```

ip pim-sparse dr-priority *<priority number>*

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the routers priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<priority number>	Specifies the priority number for the DR router. Valid range is 1 to 4,294,967,295.

Default Values

By default, the DR priority is set to 1.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the DR priority to 5:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip pim-sparse dr-priority 5
```

ip pim-sparse hello-timer *<time>*

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the time in seconds between hello transmissions. Valid range is 10 to 12,600 seconds.

Default Values

By default, the hello timer is set to 30 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the hello timer to 60 seconds:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip pim-sparse hello-timer 60
```

ip pim-sparse nbr-timeout *<time>*

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is 30 to 10,800 seconds.

Default Values

By default, the nbr-timeout is set to 105 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip pim-sparse nbr-timeout 300
```

ip pim-sparse override-interval *<time>*

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the LAN may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the delay time in milliseconds. Valid range is 0 to 65,535 milliseconds.

Default Values

By default, the override-interval is set to 2500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override-interval to 3000 milliseconds:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip pim-sparse override-interval 3000
```

ip pim-sparse propagation-delay *<time>*

Use the **ip pim-sparse propagation-delay** command to specify protocol-independent multicast (PIM) sparse join/prune propagation delay. This is the expected propagation delay in milliseconds over the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the expected propagation delay in milliseconds. Valid range is 0 to 32,767 milliseconds.

Default Values

By default, the propagation-delay is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation-delay to 1000 milliseconds:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip pim-sparse propagation-delay 1000
```

ip policy route-map *<policy name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<policy name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip policy route-map policy1
```

ip proxy-arp *<address> <subnet mask>*

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy ARP is enabled.

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

In general, the principle of proxy-arp allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, the AOS will respond to all arp requests with its specified MAC address and forward packets accordingly.

Enabling proxy-arp on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following enables proxy ARP on the Ethernet interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface.

Syntax Description

1	Accepts only RIP version 1 packets received on the interface.
2	Accepts only RIP version 2 packets received on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version [1 | 2]* on page 1144 for more information.

The AOS only accepts one version (either **1** or **2**) on a given interface.

Usage Examples

The following example configures the Ethernet interface to accept only RIP version 2 packets:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface.

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. Refer to *version [1 | 2]* on page 1144 for more information.

The AOS only transmits one version (either **1** or **2**) on a given interface.

Usage Examples

The following example configures the Ethernet interface to transmit only RIP version 2 packets:

```
(config)#interface eth 0/1
(config-eth 0/1)#ip rip send version 2
```

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> NOTE *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route-cache is enabled for all virtual PPP interfaces.

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the Ethernet interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ip route-cache
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface (in the format **type slot/port**) that contains the IP address to be used as the source address for all packets transmitted on this interface

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.
Release 6.1	Command was expanded to include VLAN interfaces.
Release 11.1	Command was expanded to include demand interfaces.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered ppp 1** while in the Ethernet Interface Configuration mode configures the Ethernet interface to use the IP address assigned to the PPP interface for all IP processing. In addition, the AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the Ethernet interface (labeled **eth 0/1**) to use the IP address assigned to the PPP interface (**ppp 1**):

```
(config)#interface eth 0/1
(config-eth 0/1)#ip unnumbered ppp 1
```

lldp receive

Use the **lldp receive** command to allow LLDP packets to be received on this interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000
and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Usage Examples

The following example configures Ethernet interface 0/1 to receive LLDP packets:

```
(config)#interface eth 0/1
(config-eth 0/1)#lldp receive
```

lldp send [management-address I port-description I system-capabilities I system-description I system-name I and-receive]

Use the **lldp send** command to configure this interface to transmit LLDP packets or to control the types of information contained in the LLDP packets transmitted by this interface.

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device’s system capabilities on this interface.
system-description	Enables transmission of this device’s system description on this interface.
system-name	Enables transmission of this device’s system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

Be default, all interfaces are configured to transmit and receive LLDP packets of all types.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures Ethernet interface 0/1 to transmit LLDP packets containing all enabled information types:

```
(config)#interface eth 0/1
(config-eth 0/1)#lldp send
```

The following example configures Ethernet interface 0/1 to transmit and receive LLDP packets containing all information types:

```
(config)#interface eth 0/1
(config-eth 0/1)#lldp send-and-receive
```

mac-address *<address>*

Use the **mac-address** command to specify the Media Access Control (MAC) address of the unit. Only the last three values of the MAC address can be modified. The first three values contain the ADTRAN reserved number (00:0A:C8) by default. Use the **no** form of this command to return to the default MAC address programmed by ADTRAN.

Syntax Description

<address>	Specifies a MAC address entered in a series of six dual-digit hexadecimal values separated by colons (for example 00:0A:C8:5F:00:D2).

Default Values

A unique default MAC address is programmed in each unit shipped by ADTRAN.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include Gigabit Ethernet interfaces.

Usage Examples

The following example configures a MAC address of **00:0A:C8:5F:00:D2**:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#mac-address 00:0A:C8:5F:00:D2
```

max-reserved-bandwidth *<percent>*

Use the **max-reserved-bandwidth** command to define the maximum amount of interface bandwidth reserved for Quality of Service (QoS). Use the **no** form of this command to return to the default value.

Syntax Description

<percent>	Specifies the maximum amount of bandwidth to reserve for QoS. This setting is configured as a percentage of the total interface speed. Range: 1 to 100 percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent.

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the **reserved-bandwidth** maximum at 80 percent:

```
(config)#interface eth 0/1
(config-eth 0/1)#max-reserved-bandwidth 80
```

mtu *<size>*

Use the **mtu** command to configure the maximum transmit unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size> Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:

ATM interfaces	64 to 1520
Demand interfaces	64 to 1520
Ethernet interfaces	64 to 1500
HDLC interfaces	64 to 1520
Loopback interfaces	64 to 1500
Tunnel interfaces	64 to 18,190
Virtual Frame Relay sub-interfaces	64 to 1520
Virtual PPP interfaces	64 to 1500

Default Values

<size> The default values for the various interfaces are listed below:

ATM interfaces	1500
Demand interfaces	1500
Ethernet interfaces	1500
HDLC interfaces	1500
Loopback interfaces	1500
Tunnel interfaces	1500
Virtual Frame Relay sub-interfaces	1500
Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1 Command was introduced.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#mtu 1200
```

qos-policy out *<mapname>*

Use the **qos-policy out** command to apply a previously-configured QoS map to an interface. Use the **no** form of this command to remove the map from the interface. The **out** keyword specifies that this policy will be applied to outgoing packets.

Syntax Description

<mapname>	Specifies the name of a previously-created QoS map (see *qos map <mapname> <sequence number>* on page 434 for more information).

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross-connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when ADSL finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#qos-policy out VOICEMAP
```

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and sub-interfaces) have SNMP traps enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Ethernet sub-interfaces and Gigabit Ethernet interfaces.

Usage Examples

The following example enables SNMP capability on the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#snmp trap
```

snmp trap link-status

Use the **snmp trap link-status** command to control the SNMP variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the interface:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#no snmp trap link-status
```

spanning-tree bpdufilter [enable | disable]

Use the **spanning-tree bpdufilter** command to enable or disable the BPDU filter on a specific interface. This setting overrides the related Global setting (refer to *spanning-tree edgeport bpdufilter default* on page 457). Use the **no** version of the command to return to the default setting.

Syntax Description

enable	Enables BPDU filter for this interface.
disable	Disables BPDU filter for this interface.

Default Values

By default, this setting is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpdufilter blocks any BPDUs from being transmitted and received on an interface.

Usage Examples

The following example enables the BPDU filter on the interface **eth 0/3**:

```
(config)#interface eth 0/3
(config-eth 0/3)#spanning-tree bpdufilter enable
```

The BPDU filter can be disabled on the **eth 0/3** by issuing the following commands:

```
(config)#interface eth 0/3
(config-eth 0/3)#spanning-tree bpdufilter disable
```

spanning-tree bpduguard [enable | disable]

Use the **spanning-tree bpduguard** command to enable or disable the BPDU guard on a specific interface. This setting overrides the related global setting (refer to *spanning-tree forward-time <seconds>* on page 460). Use the **no** version of the command to return to the default setting.

Syntax Description

enable	Enables BPDU guard for this interface.
disable	Disables BPDU guard for this interface.

Default Values

By default, this setting is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The bpduguard blocks any BPDUs from being received on an interface.

Usage Examples

The following example enables the BPDU guard on the interface **eth 0/3**:

```
(config)#interface eth 0/3
(config-eth 0/3)#spanning-tree bpduguard enable
```

The BPDU guard can be disabled on the **eth 0/3** by issuing the following commands:

```
(config)#interface eth 0/3
(config-eth 0/3)#spanning-tree bpduguard disable
```

spanning-tree edgeport

Use the **spanning-tree edgeport** command to configure the interface to be an edgeport. This command overrides the related Global setting (refer to *spanning-tree edgeport default* on page 459). Use the **no** version of the command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, this setting is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Enabling this command configures the interface to go to a forwarding state when the link becomes active. When not enabled, an interface must go through the listening and learning states before going to the forwarding state.

Usage Examples

The following example configures the interface to be an edgeport:

```
(config)#interface eth 0/1
(config-eth 0/1)#spanning-tree edgeport
```

An individual interface can be configured to not be considered an edgeport. For example:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#no spanning-tree edgeport
```

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

Use the **spanning-tree link-type** command to configure the spanning tree protocol link type for each interface. Use the **no** version of the command to return to the default setting.

Syntax Description

auto	Determines link type by the port's duplex settings.
point-to-point	Manually sets link type to **point-to-point**, regardless of duplex settings.
shared	Manually sets link type to **shared**, regardless of duplex settings.

Default Values

By default, the interface is set to auto.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command overrides the default link type setting determined by the duplex of the individual port. By default, a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Use the **link-type auto** command to restore the convention of determining link type based on duplex settings.

Technology Review

Rapid transitions are possible in rapid spanning-tree protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link-type to **auto** allows the spanning-tree to automatically configure the link type based on the duplex of the link. Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

Usage Examples

The following example forces the link type to **point-to-point**, even if the port is configured to be half-duplex:

```
(config)#interface eth 0/3
(config-eth 0/3)#spanning-tree link-type point-to-point
```

spanning-tree pathcost method [short | long]

Use the **spanning-tree pathcost** command to select a short or long method used by the spanning-tree protocol.

Syntax Description

short	Specifies 16-bit values when calculating pathcosts.
long	Specifies 32-bit values when calculating pathcosts.

Default Values

By default, **spanning-tree pathcost** is set to **short**.

Applicable Platforms

This command applies to the NetVanta 1000, 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example specifies that the spanning tree protocol use a long pathcost method:

```
(config)#spanning-tree pathcost method long
```

spanning-tree port-priority *<priority level>*

Use the **spanning-tree port-priority** command to select the priority level of this interface. To return to the default setting, use the **no** version of this command.

Syntax Description

<priority level>	Specifies a value from 0 to 255.

Default Values

By default, this set to 128.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The only time that this priority level is used is when two interfaces with a path to the root have equal cost. At that point, the level set in this command will determine which port the spanning tree will use. Set the priority value lower to increase the chance the interface will be used.

Usage Examples

The following example sets the interface to a priority of 100:

```
(config)#interface eth 0/3
(config-eth 0/3)#spanning-tree port-priority 100
```

speed [10 | 100 | auto | nonegotiate]

Use the **speed** command to configure the speed of an Ethernet interface. Use the **no** form of this command to return to the default value.

Syntax Description

10	Specifies 10 Mbps Ethernet.
100	Specifies 100 Mbps Ethernet.
auto	Automatically detects 10 or 100 Mbps Ethernet and negotiates the duplex setting.
nonegotiate	Disables auto negotiation and forces the speed to 1 Gbps. This only applies to Gigabit Ethernet interfaces.

> NOTE *If the **speed** is manually set to **10** or **100,** the duplex must be manually configured as **full-duplex** or **half-duplex**.*

Default Values

By default, speed is set to auto.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the Ethernet port for 100 Mb operation:

```
(config)#interface ethernet 0/1
(config-eth 0/1)#speed 100
```

traffic-shape rate *<rate> <burstrate>*

Use the **traffic-shape rate** command to specify and enforce an output bandwidth for Ethernet and VLAN interfaces.

Syntax Description

<rate>	Specifies the rate (in bits per second) at which the interface should be shaped.
<burstrate>	Optional. Specifies the allowed burst in bytes. By default, this is specified to the rate divided by 5 to represent the number of bytes that would flow within 200 ms.

Default Values

By default, traffic-shaping rate is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Functional Notes

Traffic shaping can be used to limit an Ethernet segment to a particular rate or to specify use of QoS on Ethernet or VLAN interfaces.

Usage Examples

The following example sets the outbound rate of **eth 0/1** to 128 kbps and applies a QoS policy that all RTP traffic is given priority over all other traffic:

```
(config)#qos map voip 1
(config-qos-map)#match ip rtp 10000 10500 all
(config-qos-map)#priority unlimited
(config-qos-map)#interface eth 0/1
(config-eth)#traffic-shape rate 128000
(config-eth)#qos-policy out voip
```

vlan-id *<vlan id>* [native]

Use the **vlan-id** command to set a VLAN ID for the Ethernet interface. Use the **no** form of this command to remove an entry.

Syntax Description

<vlan id >	Specifies a valid VLAN interface ID number (1 to 4095).
native	Optional. Specifies that data for that VLAN ID goes out untagged. If **native** is not specified, data for that VLAN ID goes out tagged.

Default Values

By default, no VLAN ID is set.

Applicable Platforms

This command applies to the NetVanta 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example configures a native VLAN of 5 for the Ethernet interface 0/1:

```
(config)#interface eth 0/1
(config-eth 0/1)#vlan-id 5 native
```

G.703 INTERFACE CONFIGURATION COMMAND SET

To activate the G.703 Interface Configuration mode, enter the **interface e1** command (and specify the G.703 port) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface e1 1/2
(config-e1 1/2)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

coding [ami | hdb3] on page 593

framing [crc4] on page 594

loopback network [line | payload] on page 595

snmp trap link-status on page 596

test-pattern [ones | zeros] on page 597

ts16 on page 598

coding [ami | hdb3]

Use the **coding** command to configure the line coding for the G.703 physical interface. This setting must match the line coding supplied on the circuit by the PBX.

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
hdb3	Configures the line coding for high-density bipolar 3 (HDB3).

Default Values

By default, all E1 interfaces are configured with HDB3 line coding.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the E1 circuit. A mismatch will result in line errors (e.g., BPVs).

Usage Examples

The following example configures the G.703 interface for AMI line coding:

```
(config)#interface e1 1/2
(config-e1 1/2)#coding ami
```

framing [crc4]

Use the **framing** command to configure the framing format for the G.703 interface. This parameter should match the framing format set on the external device. Use the **no** form of this command to return to the default value.

Syntax Description

crc4	Enables CRC4 bits to be transmitted in the outgoing data stream. Also, the received signal is checked for CRC4 errors.

Default Values

By default, CRC4 is enabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The framing value must match the configuration of the E1 circuit. A mismatch will result in a loss of frame alarm.

Usage Examples

The following example configures the G.703 interface for CRC4 framing:

```
(config)#interface e1 1/2
(config-e1 1/2)#framing crc4
```

loopback network [line | payload]

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback.

Syntax Description

line	Initiates a metallic loopback of the physical E1 network interface.
payload	Initiates a loopback of the E1 framer (CSU portion) of the E1 network interface.

Default Values

No default necessary for this command.

Applicable Platforms

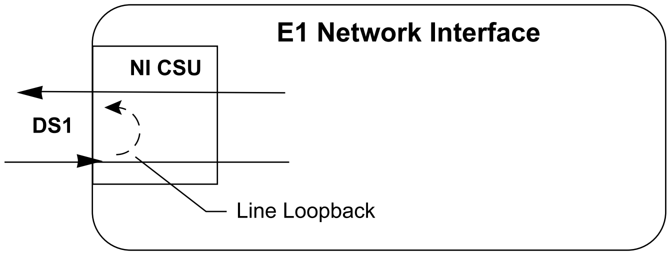
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The following diagram depicts a line loopback.



Usage Examples

The following example initiates a line loopback of the G.703 interface:

```
(config)#interface e1 1/2
(config-e1 1/2)#loopback network line
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC 2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the G.703 interface:

```
(config)#interface e1 1/2
(config-e1 1/2)#no snmp trap link-status
```

test-pattern [ones | zeros]

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation.

Syntax Description

ones	Generates a test pattern of continous ones.
zeros	Generates a test pattern of continous zeros.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.
Release 6.1	Command was expanded to include E1 and G.703 interfaces.

Usage Examples

The following example activates the pattern generator for a stream of continuous ones:

```
(config)#interface e1 1/2
(config-e1 1/2)#test-pattern ones
```

ts16

Use the **ts16** command to enable timeslot 16 multiframe to be checked on the receive signal. Use the **no** form of this command to disable timeslot 16.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables timeslot 16 multiframing:

```
(config)#interface e1 1/2
(config-e1 1/2)#ts16
```

HSSI INTERFACE CONFIGURATION COMMAND SET

To activate the HSSI Interface Configuration mode, enter the **interface hssi** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface hssi 1/1
(config-hssi 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

external-loopback-request on page 600

loopback [dce | dte | line | remote | none] on page 601

snmp trap link-status on page 602

external-loopback-request

Use the **external-loopback-request** command to enable LC (loopback circuit C) input to control loopbacks toward the network. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables the unit to accept external loopback requests:

```
(config)#interface hssi 1/1
(config-hssi 1/1)#external-loopback-request
```

loopback [dce | dte | line | remote | none]

Use the **loopback** command to initiate or remove a loopback.

Syntax Description

dce	Initiates a loopback on the DCE.
dte	Initiates a loopback on the DTE.
line	Initiates a local line loopback.
remote	Initiates a remote line loopback.
none	Removes an active loopback.

Default Values

By default, no loopbacks are active.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example initiates a local line loopback on the HSSI interface:

```
(config)#interface hssi 1/1
(config-hssi 1/1)#loopback line
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap..

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.
Release 7.1	Command was extended to include the HSSI interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the interface:

```
(config)#interface hssi 1/1
(config-hssi 1/1)#no snmp trap link-status
```

T1 Interface Configuration Command Set

To activate the T1 Interface Configuration mode, enter the **interface t1** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface t1 1/1
(config-t1 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

clock source [internal | line | through | through <interface id>] on page 604

coding [ami | b8zs] on page 605

fdl [ansi | att | none] on page 606

framing [d4 | esf] on page 607

lbo [long <-22.5, -15, -7.5, 0> | short <0-655>] on page 608

loopback commands begin on page 609

remote-alarm [rai] on page 612

remote-loopback on page 613

show test-pattern on page 614

snmp trap line-status on page 615

snmp trap link-status on page 616

snmp trap threshold-reached on page 617

tdm-group <group number> timeslots <1-24> speed [56 | 64] on page 618

test-pattern [clear | insert | ones | p215 | p220 | p511 | qrss | zeros] on page 619

clock source [internal | line | through | through *<interface id>*]

Use the **clock source** command to configure the source timing used for the interface. Use the **no** form of this command to return to the default value.

Syntax Description

internal	Configures the unit to provide clocking using the internal oscillator.
line	Configures the unit to recover clocking from the T1 circuit.
through	Configures the unit to recover clocking from the circuit connected to the DSX-1 interface.
through t1 *<interface id>*	Configures the unit to recover clocking from the alternate interface. Only valid on T1 systems with multiple T1 interfaces and a single clock source.

Default Values

By default, the **clock source** is set to **line**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

When operating on a circuit that is providing timing, setting the **clock source** to **line** can avoid errors such as Clock Slip Seconds (CSS).

Usage Examples

The following example configures the unit to recover clocking from the primary circuit:

```
(config)#interface t1 1/1
(config-t1 1/1)#clock source line
```

coding [ami | b8zs]

Use the **coding** command to configure the line coding for a T1 physical interface. This setting must match the line coding supplied on the circuit by the service provider.

Syntax Description

ami	Configures the line coding for alternate mark inversion (AMI).
b8zs	Configures the line coding for bipolar eight zero substitution (B8ZS).

Default Values

By default, all T1 interfaces are configured with B8ZS line coding.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the T1 circuit. A mismatch will result in line errors (e.g., BPVs).

Usage Examples

The following example configures the T1 interface for AMI line coding:

```
(config)#interface t1 1/1
(config-t1 1/1)#coding ami
```

fdl [ansi | att | none]

Use the **fdl** command to configure the format for the facility data link (FDL) channel on the T1 circuit. FDL channels are only available on point-to-point circuits. Use the **no** form of this command to return to the default value.

Syntax Description

ansi	Configures the FDL for ANSI T1.403 standard.
att	Configures the FDL for AT&T TR 54016 standard.
none	Disables FDL on this circuit.

Default Values

By default, the FDL is configured for **ansi**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

T1 circuits using ESF framing format (specified using the **framing** command) reserve 12 bits as a data link communication channel, referred to as the FDL, between the equipment on either end of the circuit. The FDL allows the transmission of trouble flags such as the Yellow Alarm signal. Refer to *framing [d4 | esf]* on page 607 for related information.

Usage Examples

The following example disables the FDL channel for the T1 circuit:

```
(config)#interface t1 1/1
(config-t1 1/1)#fdl none
```

framing [d4 | esf]

Use the **framing** command to configure the framing format for the T1 interface. This parameter should match the framing format supplied by your network provider. Use the **no** form of this command to return to the default value.

Syntax Description

d4	Specifies D4 superframe (SF) format.
esf	Specifies extended superframe (ESF) format.

Default Values

By default, the framing format is set to **esf**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

A frame is comprised of a single byte from each of the T1's timeslots; there are 24 timeslots on a single T1 circuit. Framing bits are used to separate the frames and indicate the order of information arriving at the receiving equipment. D4 and ESF are two methods of collecting and organizing frames over the circuit.

Usage Examples

The following example configures the T1 interface for D4 framing:

```
(config)#interface t1 1/1
(config-t1 1/1)#framing d4
```

lbo [long *<-22.5, -15, -7.5, 0>* | short *<0-655>*]

Use the **lbo** command to configure the line build out (LBO) for the T1 interface. Use the **no** form of this command to return to the default value.

Syntax Description

long *<-22.5, -15, -7.5, 0>* Configures the LBO (in dB) for T1 interfaces with cable lengths greater than 655 feet. Choices are -22.5, -15, -7.5, and 0 dB.

short *<0-655>* Configures the LBO (in feet) for T1 interfaces with cable lengths less than 655 feet. Range is 0 to 655 feet.

Default Values

By default, the build out is set to 0 dB.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1 Command was introduced.

Functional Notes

Line build out (LBO) is artificial attenuation of a T1 output signal to simulate a degraded signal. This is useful to avoid overdriving a receiver's circuits. The shorter the distance between T1 equipment (measured in cable length), the greater the attenuation value. For example, two units in close proximity should be configured for the maximum attenuation (-22.5 dB).

Usage Examples

The following example configures the T1 interface LBO for -22.5 dB:

```
(config)#interface t1 1/1
(config-t1 1/1)#lbo -22.5
```

loopback network [line | payload]

Use the **loopback network** command to initiate a loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback.

Syntax Description

line	Initiates a metallic loopback of the physical T1 network interface.
payload	Initiates a loopback of the T1 framer (CSU portion) of the T1 network interface.

Default Values

No default necessary for this command.

Applicable Platforms

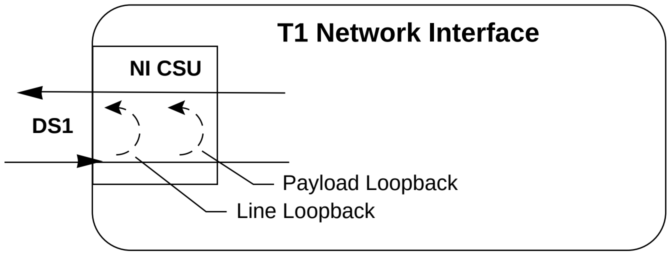
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a payload loopback of the T1 interface:

```
(config)#interface t1 1/1
(config-t1 1/1)#loopback network payload
```

loopback remote line [fdl | inband]

Use the **loopback remote line** command to send a loopback code to the remote unit to initiate a line loopback. Use the **no** form of this command to send a loopdown code to the remote unit to deactivate the loopback.

Syntax Description

fdl	Uses the facility data link (FDL) to initiate a full 1.544 Mbps physical (metallic) loopback of the signal received by the remote unit from the network.
inband	Uses the inband channel to initiate a full 1.544 Mbps physical (metallic) loopback of the signal received by the remote unit from the network.

Default Values

No defaults necessary for this command.

Applicable Platforms

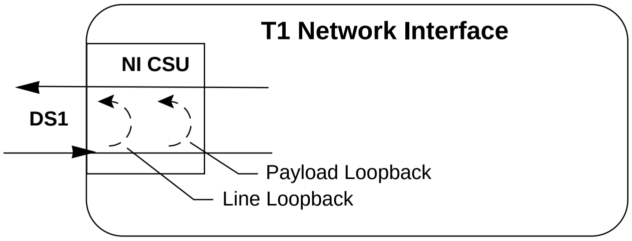
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a remote line loopback using the FDL:

```
(config)#interface t1 1/1
(config-t1 1/1)#loopback remote line fdl
```

loopback remote payload

Use the **loopback remote payload** command to send a loopback code to the remote unit to initiate a payload loopback. A payload loopback is a 1.536 Mbps loopback of the payload data received from the network maintaining bit-sequence integrity for the information bits by synchronizing (regenerating) the timing. Use the **no** form of this command to send a loopdown code to the remote unit to deactivate the loopback.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

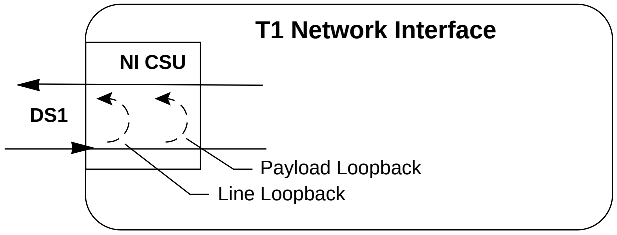
This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The following diagram depicts the difference between a line and payload loopback.



Usage Examples

The following example initiates a remote payload loopback:

```
(config)#interface t1 1/1
(config-t1 1/1)#loopback remote payload
```

remote-alarm [rai]

The **remote-alarm** command selects the alarm signaling type to be sent when a loss of frame is detected on the T1 receive signal. Use the **no** form of this command to disable all transmitted alarms.

Syntax Description

rai	Specifies sending a remote alarm indication (RAI) in response to a loss of frame. Also prevents a received RAI from causing a change in interface operational status.

Default Values

The default for this command is **rai**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was expanded to include the T1 interface.

Usage Examples

The following example enables transmission of RAI in response to a loss of frame:

```
(config)#interface t1 1/1
(config-t1 1/1)#remote-alarm rai
```

remote-loopback

Use the **remote-loopback** command to configure the interface to respond to loopbacks initiated by a remote unit (or the service provider). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Values

By default, all interfaces respond to remote loopbacks.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables remote loopbacks on the T1 interface:

```
(config)#interface t1 1/1
(config-t1 1/1)#remote-loopback
```

show test-pattern

Use the **show test-pattern** command to display results from test patterns inserted using the **test-pattern** command (refer to *test-pattern [clear | insert | ones | p215 | p220 | p511 | qrss | zeros]* on page 619 for more information).

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following is sample output from this command:

```
(config)#interface t1 1/1
(config-t1 1/1)#show test-pattern
QRSS Errored Seconds: 6
```

snmp trap line-status

Use the **snmp trap line-status** command to control the Simple Network Management Protocol (SNMP) variable dsx1LineStatusChangeTrapEnable (RFC2495) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the dsx1LineStatusChangeTrapEnable OID is set to enabled for all interfaces except virtual Frame Relay Interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **snmp trap line-status** command is used to control the RFC2495 dsx1LineStatusChangeTrapEnable OID (OID number 1.3.6.1.2.1.10.18.6.1.17.0).

Usage Examples

The following example disables the line-status trap on the T1 interface:

```
(config)#interface t1 1/1
(config-t1 1/1)#no snmp trap line-status
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the T1 interface:

```
(config)#interface t1 1/1
(config-t1 1/1)#no snmp trap link-status
```

snmp trap threshold-reached

Use the **snmp trap threshold-reached** command to control the Simple Network Management Protocol (SNMP) variable adGenAOSDs1ThresholdReached (adGenAOSDs1-Ext MIB) to enable the interface to send SNMP traps when a DS1 performance counter threshold is reached. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the adGenAOSDs1ThresholdReached OID is enabled for all interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example disables SNMP threshold reached trap on the T1 interface:

```
(config)#interface t1 1/1
(config-t1 1/1)#no snmp trap threshold-reached
```

tdm-group *<group number>* timeslots *<1-24>* speed [56 | 64]

Use the **tdm-group** command to create a group of contiguous DS0s on this interface to be used during the **cross-connect** process. Refer to *crypto map <mapname>* on page 896 for related information.

> CAUTION *Changing **tdm-group** settings could result in service interruption.*

Syntax Description

<group number>	Identifies the created TDM group (valid range: 1 to 255).
timeslots *<1-24>*	Specifies the DS0s to be used in the TDM group. This can be entered as a single number representing one of the 24 T1 channel timeslots or as a contiguous group of DS0s. (For example, **1-10** specifies the first 10 channels of the T1.)
speed [56 | 64]	Optional. Specifies the individual DS0 rate on the T1 interface to be 64 kbps. Only the T1 + DSX-1 Network Interface Module supports the 56 kbps DS0 rate. The default speed is 64 kbps.

Default Values

By default, there are no configured TDM groups.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example creates a TDM group (labeled **5**) of 10 DS0s at 64 kbps each:

```
(config)#interface t1 1/1
(config-t1 1/1)#tdm-group 5 timeslots 1-10 speed 64
```

test-pattern [clear | insert | ones | p215 | p220 | p511 | qrss | zeros]

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the specified test pattern. This pattern generation can be used to verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation.

Syntax Description

clear	Clears the test pattern error count.
insert	Inserts an error into the currently active test pattern. Display the injected error result using the **show test pattern** command.
ones	Generates a test pattern of continous ones.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.
p220	Generates a pseudorandom test pattern sequence based on a 20-bit shift register.
p511	Generates a test pattern of repeating ones and zeros.
qrss	Generates a test pattern of random ones and zeros.
zeros	Generates a test pattern of continous zeros.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example activates the pattern generator for a stream of continuous ones:

```
(config)#interface t1 1/1
(config-t1 1/1)#test-pattern ones
```

T3 INTERFACE CONFIGURATION COMMAND SET

To activate the T3 Interface Configuration mode, enter the **interface t3** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface t3 1/1
(config-t3 1/1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

clock source [local | loop] on page 621

coding [b3zs] on page 622

framing [m13 | cbit] on page 623

line-length [short | long] on page 624

loopback network [line | payload] on page 625

loopback remote [line | payload] on page 626

remote-loopback on page 627

show [bert] on page 628

snmp trap link-status on page 629

test-pattern [clear | insert | ones | p215 | p223 | zeros] on page 630

clock source [local | loop]

Use the **clock source** command to configure the source timing used for the interface. The clock specified using the **clock source** command is also the system master clock. Use the **no** form of this command to return to the default value.

Syntax Description

local	Configures the unit to provide clocking using the internal oscillator.
loop	Configures the unit to recover clocking from the T3 circuit.

Default Value

By default, all T3 interfaces are configured with loop as the clock source.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Example

The following example configures the unit to recover clocking from the circuit:

```
(config)#interface t3 1/1
(config-t3 1/1)#clock source loop
```

coding [b3zs]

Use the **coding** command to configure the line coding for a T3 physical interface. This setting must match the line coding supplied on the circuit by the service provider.

Syntax Description

b3zs	Configures the line coding for bipolar three zero substitution (B3ZS).

Default Value

By default, all T3 interfaces are configured with B3ZS line coding.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Functional Notes

The line coding configured in the unit must match the line coding of the T3 circuit. A mismatch will result in line errors (e.g., BPVs).

Usage Example

The following example configures the T1 interface for B3ZS line coding:

```
(config)#interface t3 1/1
(config-t3 1/1)#coding b3zs
```

framing [m13 | cbit]

Use the **framing** command to configure the network framing format for a T3 physical interface.

Syntax Description

m13	Configures the interface for M13 framing.
cbit	Configures the interface for C-bit parity framing.

Default Value

By default, all T3 interfaces are configured for C-bit parity framing.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Functional Notes

M13 is an asynchronous framing format that uses all 21 DS3 M-Frame C-bits for bit stuffing indicators. End-to-end path parity and datalink capabilities are not provided by the standard M13 format. C-bit parity framing differs from M13 by allowing monitoring of the data path (end-to-end) and supporting out-of-band data links.

Usage Example

The following example configures the T3 interface for M13 framing:

```
(config)#interface t3 1/1
(config-t3 1/1)#framing m13
```

line-length [short | long]

Use the **line-length** command to configure the line length for a T3 physical interface.

Syntax Description

short	Configures the line length for a distance of 0 to 225 feet of cable.
long	Configures the line length for a distance of 225 to 450 feet of cable.

Default Value

By default, all T3 interfaces are configured for a short line length.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example configures the T3 interface for long line length:

```
(config)#interface t3 1/1
(config-t3 1/1)#line-length long
```

loopback network [line | payload]

Use the **loopback network** command to initiate a local T3 loopback on the interface toward the network. Use the **no** form of this command to deactivate the loopback.

Syntax Description

line	Initiates a loopback of the physical T3 network interface; that is, data received on the T3 is transmitted back out on the T3.
payload	Initiates a loopback of the T3 framer (TSU portion) of the T3 network interface.

Default Value

No default necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Example

The following example initiates a payload loopback of the T3 interface:

```
(config)#interface t3 1/1
(config-t3 1/1)#loopback network payload
```

loopback remote [line | payload]

Use the **loopback remote** command to initiate a loopback test on the T3 interface that sends a remote loopback code out the T3 circuit to loop up the far end. This command only applies when C-bit framing is used on the circuit. Use the **no** form of this command to deactivate the loopback.

Syntax Description

line	Initiates a line loopback.
payload	Initiates a payload loopback.

Default Value

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Examples

This example initiates a remote loopback on the T3 interface:

```
(config)#interface t3 1/1
(config-t3 1/1)#loopback remote
```

remote-loopback

Use the **remote-loopback** command to configure the T3 interface to be looped *from* the far end (remote device, telco, etc.). Use the **no** form of this command to disable this feature.

Syntax Description

No subcommands.

Default Value

By default, all interfaces respond to remote loopbacks.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Examples

This example enables remote loopbacks on the T3 interface:

```
(config)#interface t3 1/1
(config-t3 1/1)#remote-loopback
```

show [bert]

The **show bert** command displays the results for the bit error rate test (BERT) conducted on the T3 interface.

Syntax Description

No subcommands.

Default Value

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example instructs the unit to display the BERT results:

```
(config)#interface t3 1/1
(config-t3 1/1)#show bert
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Value

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Example

The following example disables the link-status trap on the T3 interface:

```
(config)#interface t3 1/1
(config-t3 1/1)#no snmp trap link-status
```

test-pattern [clear | insert | ones | p215 | p223 | zeros]

Use the **test-pattern** command to activate the built-in pattern generator and begin sending the selected test pattern toward the network. This pattern generation can verify a data path when used in conjunction with an active loopback. Use the **no** form of this command to cease pattern generation.

Syntax Description

clear	Clears the test pattern error count.
insert	Inserts an error into the currently active test pattern. Display the injected error result using the **show test pattern** command.
ones	Generates a test pattern of continous ones.
p215	Generates a pseudorandom test pattern sequence based on a 15-bit shift register.
p223	Generates a pseudorandom test pattern sequence based on a 23-bit shift register.
zeros	Generates a test pattern of continous zeros.

Default Value

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 5000 Series.

Command History

Release 6.1	Command was introduced.

Usage Example

The following example inserts a p215 test pattern:

```
(config)#interface t3 1/1
(config-t3 1/1)#test-pattern 2^15 insert
```

DEMAND INTERFACE CONFIGURATION COMMAND SET

To activate the Demand Interface Configuration mode, enter the **interface demand** command at the Global Configuration mode prompt. For example:

```
#configure terminal
(config)#interface demand 1
(config-demand 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 633

bandwidth <value> on page 636

called-number <DNIS number> on page 637

caller-number <CLID number> on page 638

connect-mode [answer | originate | either] on page 639

connect-order [last-successful | round-robin | sequential] on page 640

connect-sequence on page 641

connect-sequence attempts <value> on page 643

connect-sequence interface-recovery [retry-interval <seconds> | max-retries <value>] on page 644

crypto map <mapname> on page 645

demand-hold-queue <packets> timeout <seconds> on page 647

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 648

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic to an interface. Use the **no** form of this command to remove an access policy association.

> NOTE *Configured access policies will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<policyname>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 2.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** *<policy name>*.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the virtual PPP interface:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:

```
(config)#ip policy-class UnTrusted
(config-policy-class)#allow list InWeb
```

Associate the access list with the demand virtual interface (labeled 1):

```
(config)#interface demand 1
(config-demand 1)#access-policy UnTrusted
```

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:

Enable the security features of the AOS using the **ip firewall** command.

Step 2:

Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:

Create an access policy that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>

All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>

All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the virtual PPP interface labeled 1:

```
(config)#interface demand 1
(config-demand 1)#access-policy MatchAll
```

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies the bandwidth value in kbps.

Default Values

To view default values, use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets the bandwidth of the demand interface to 10 Mbps:

```
(config)#interface demand 1
(config-demand 1)#bandwidth 10000
```

called-number *<DNIS number>*

Use the **called-number** command to link calls to specific interfaces based on their dialed number identification service (DNIS) numbers. Multiple called numbers may be specified for an interface. Use the **no** form of this command to restore the default values.

Syntax Description

<DNIS number>	Identifies the called number to be linked to an interface. The DNIS number is limited to 20 digits.

Default Values

By default no called numbers are defined.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example links calls with a DNIS number of **2565558409** to the demand interface **1**:

```
(config)#interface demand 1
(config-demand 1)#called-number 2565558409
```

caller-number *<CLID number>*

Use the **caller-number** command to link calls to specific interfaces based on it's caller ID (CLID) number. Multiple caller ID numbers may be specified, allowing the interface to accept calls from different remote resources. Use the **no** form of this command to restore the default values.

Syntax Description

<CLID number>	Identifies the caller's number to be linked to an interface. The CLID number is limited to 20 digits.

Default Values

By default, no caller numbers are defined.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example links calls with a CLID number of **2565559911** to the demand interface **1**:

```
(config)#interface demand 1
(config-demand 1)#caller-number 2565559911
```

connect-mode [answer | originate | either]

Use the **connect-mode** command to configure the interface to only answer calls, only originate calls, or to both answer and originate calls. Use the **no** form of this command to restore the default values.

Syntax Description

answer	Specifies the interface may be used to answer calls but not originate calls.
originate	Specifies the interface may be used to originate calls but not answer calls.
either	Specifies the interface may be used to answer and originate calls.

Default Values

By default the connect mode is set to both answer and originate calls.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to only answer calls:

```
(config)#interface demand 1
(config-demand 1)#connect-mode answer
```

connect-order [last-successful | round-robin | sequential]

Use the **connect-order** command to specify the starting point in the connection sequence for each sequence activation. The connection sequence is a circular list. Use the **no** form of this command to restore the default values.

Syntax Description

last-successful	Specifies the connect sequence be processed beginning with the last successful entry or the first entry if there are no previous connections.
round-robin	Specifies the connect sequence be processed beginning with the entry that follows the last successful entry or the first entry if there are no previous connections.
sequential	Specifies the connect sequence be processed from the beginning of the list.

Default Values

By default, connect sequences are processed sequentially.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures the connection sequence to begin with the last successful entry:

```
(config)#interface demand 1
(config-demand 1)#connect-order last-successful
```

connect-sequence

Use the **connect-sequence** command to provide instructions to the interface on how to use the resource pool and telephone numbers to connect to demand destinations. Use the **no** form of this command to restore the default values.

Variations of this command include the following:

connect-sequence <*sequence number*> **dial-string** <*string*> **forced-analog**
connect-sequence <*sequence number*> **dial-string** <*string*> **forced-analog busyout-threshold** <*value*>
connect-sequence <*sequence number*> **dial-string** <*string*> **forced-isdn-56k**
connect-sequence <*sequence number*> **dial-string** <*string*> **forced-isdn-56k**
  busyout-threshold <*value*>
connect-sequence <*sequence number*> **dial-string** <*string*> **forced-isdn-64k**
connect-sequence <*sequence number*> **dial-string** <*string*> **forced-isdn-64k**
  busyout-threshold <*value*>
connect-sequence <*sequence number*> **dial-string** <*string*> **isdn-56k**
connect-sequence <*sequence number*> **dial-string** <*string*> **isdn-56k busyout-threshold** <*value*>
connect-sequence <*sequence number*> **dial-string** <*string*> **isdn-64k**
connect-sequence <*sequence number*> **dial-string** <*string*> **isdn-64k busyout-threshold** <*value*>

Syntax Description

<*sequence number*>	Specifies the number for this connection specification entry. Range: 1 to 65,535.
<*string*>	Specifies the telephone number to dial when using this connection. The dial string is limited to 20 digits.
forced-analog	Specifies that only analog resources may be used.
forced-isdn-56k	Specifies that only ISDN resources may be used. Call is placed using ISDN 56k.
forced-isdn-64k	Specifies that only ISDN resources may be used. Call is placed using ISDN 64k.
isdn-56k	Specifies any dial resource may be used if ISDN 56k call-type is used.
isdn-64k	Specifies any dial resource may be used if ISDN 64k call-type is used.
busy-threshold <*value*>	Optional. Specifies the maximum number of connect sequence cycles during a activation attempt that must fail before it is skipped until the next activation attempt.

Default Values

By default any dial resource may be used.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs demand interface **1** to place the call using ISDN 64k:

```
(config)#interface demand 1
(config-demand 1)#connect-sequence 65 dial-string 2565559911 forced-isdn-64k
```

connect-sequence attempts *<value>*

Use the **connect-sequence attempts** command to limit the number of times the connect sequence will cycle when its entries are unable to establish a connection. When the maximum number of attempts are exhausted, the interface will go into recovery mode. Refer to *connect-sequence interface-recovery [retry-interval <seconds> | max-retries <value>]* on page 644 for more information. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies the number of times the connect sequence will cycle through its entries if it is unable to make a connection. Range is 0 to 65,535.

Default Values

By default the connect-sequence attempts are unlimited.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs demand interface **1** to attempt its connection sequence **500** times:

```
(config)#interface demand 1
(config-demand 1)#connect-sequence attempts 500
```

connect-sequence interface-recovery [retry-interval *<seconds>* | max-retries *<value>*]

Use the **connect-sequence interface-recovery** command to allow the interface to go down in the event that the **connect-sequence attempts** value is exhausted. Refer to *connect-sequence attempts <value>* on page 643 for more information. Use the **no** form of this command to restore the default values.

Syntax Description

retry-interval *<seconds>*	Optional. Specifies the number of seconds the interface will wait between connect sequence cycles during recovery attempts.
max-retries *<value>*	Optional. Specifies the maximum number of times the connect sequence will cycle in an attempt to bring the interface back up. When in interface recovery mode, this value overrides the **connect-sequence attempts** value.

Default Values

By default, the **connect-sequence interface-recovery retry-interval** is set to 120 seconds and **max-retries** are unlimited.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to wait **60** seconds between retry attempts with a maximum number of **500** retries:

```
(config)#interface demand 1
(config-demand 1)#connect-sequence interface-recovery retry-interval 60 max-retries 500
```

crypto map *<mapname>*

Use the **crypto map** command to associate crypto maps with the interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> NOTE *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

<mapname>	Assigns a crypto map name to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

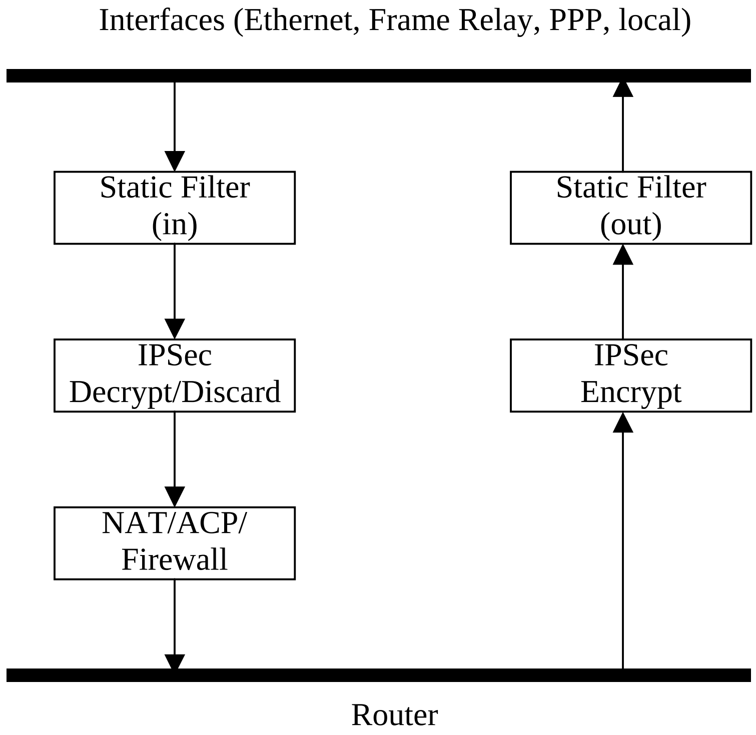
Command History

Release 4.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following notes in mind.

When defining the policy class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local-side, unencrypted source of the data. The destination information will be the far end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the demand interface:

```
(config)#interface demand 1
(config-demand 1)#crypto map MyMap
```

demand-hold-queue *<packets>* **timeout** *<seconds>*

Use the **demand-hold-queue timeout** command to set the number and length of time interesting packets will be held while a connection is being made. Use the **no** form of this command to restore the default values.

Syntax Description

<packets>	Specifies the number of packets that may be stored in the hold queue. Range is 0 to 100.
<seconds>	Specifies the number of seconds a packet may remain in the hold queue. Range is 0 to 255 seconds.

Default Values

By default, the hold queue is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to hold **50** packets in the queue for up to **120** seconds:

```
(config)#interface demand 1
(config-demand 1)#demand-hold-queue 50 timeout 120
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

Refer to *Functional Notes,* below, for argument descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 8.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or power users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service, in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address doesn't change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name) Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com) you need Custom DNS service which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the **dynamic-dns** to **dyndns-custom** with hostname **host**, username **user**, and password **pass**:

```
(config)#interface demand 1
(config-demand 1)#dynamic-dns dyndns-custom host user pass
```

fair-queue *<threshold>*

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable FIFO queueing for an interface. WFQ is enabled by default for WAN interfaces.

Syntax Description

<threshold>	Optional. Specifies the maximum number of packets that can be present in each conversation sub-queue. Packets received for a conversation after this limit is reached are discarded. Range: 16 to 512 packets.

Default Values

By default, **fair-queue** is enabled with a threshold of 64 packets.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

```
(config)#interface demand 1
(config-demand 1)#fair-queue 100
```

fast-idle *<seconds>*

Use the **fast-idle** command to set the amount of time the demand interface connection will remain active in the absence of interesting traffic when there is contention for the demand resources being used by this interface. Use the **no** form of this command to restore the default values.

Syntax Description

<seconds>	Specifies the number of seconds the interface will remain up in the absence of interesting traffic. Range is 1 to 2,147,483.

Default Values

By default, **fast-idle** is set to 120 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets fast idle to 1,073,752 seconds:

```
(config)#interface demand 1
(config-demand 1)#fast-idle 1073752
```

hold-queue *<queue size>* **out**

Use the **hold-queue out** command to change the overall size of an interface's WAN output queue.

Syntax Description

<queue size>	Specifies the total number of packets the output queue can contain before packets are dropped. Range is 16 to 1000.

Default Values

The default queue size for WFQ is 400. The default queue size for PPP FIFO and Frame Relay round-robin is 200.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example sets the overall output queue size to **700**:

```
(config)#interface demand 1
(config-demand 1)#hold-queue 700 out
```

idle-timeout *<seconds>*

Use the **idle-timeout** command to set the amount of time the interface link/bundle will remain up in the absence of interesting traffic. Interesting traffic and direction logic are set using the **match-interesting** commands. Refer to *match-interesting [list <acl name> | reverse list <acl name>] [in | out]* on page 677 for more information. Use the **no** form of this command to restore the default values.

Syntax Description

<seconds>	Specifies the number of seconds the interface will remain up in the absence of interesting traffic. Range is 1 to 2,147,483.

Default Values

By default, **idle-timeout** is set to 120 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example configures demand interface **1** to time out after **360** seconds:

```
(config)#interface demand 1
(config-demand 1)#idle-timeout 360
```

ip access-group *<listname>* [in | out]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Indicates the assigned IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into the demand interface:

```
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#interface demand 1
(config-demand 1)#ip access-group TelnetOnly in
```

ip address negotiated [no-default]

Use the **ip address negotiated** command to allow the interface to negotiate (i.e., be assigned) an IP address from the far end PPP connection. Use the **no** form of this command to disable the negotiation for an IP address

Syntax Description

no-default	Optional. Prevents the insertion of a default route. Some systems already have a default route configured and need a static route to the PPP interface to function correctly.

Default Values

By default, the interface is assigned an address with the **ip address** *<address><mask>* command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 5.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example enables the demand interface to negotiate an IP address from the far end connection:

```
(config)#interface demand 1
(config-demand 1)#ip address negotiated
```

The following example enables the demand interface to negotiate an IP address from the far end connection without inserting a default route:

```
(config)#interface demand 1
(config-demand 1)#ip address negotiated no-default
```

ip address *<address> <mask>* secondary

Use the **ip address** command to define an IP address on the specified interface. Use the optional keyword **secondary** to define a secondary IP address. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<mask>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Configures a secondary IP address for the specified interface.

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

Use secondary IP addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IP addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IP addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IP address of **192.22.72.101/30**:

```
(config)#interface demand 1
(config-demand 1)#ip address 192.22.72.101 255.255.255.252 secondary
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure the AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <port number>* on page 378 *for more information.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets.

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

```
(config)#ip forward-protocol udp domain
(config)#interface demand 1
(config-demand 1)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description	
immediate-leave	If only one host (or IGMP snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval <*milliseconds*>	Controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65535 ms. Default: 1000 ms.
querier-timeout <*seconds*>	Specifies the number of seconds that the router waits after the current querier’s last query before it takes over as querier (IGMP V2). Range: 60 to 300 seconds. Default: 2x the **query-interval** value.
query-interval <*seconds* >	Specifies the interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65,535 seconds. Default: 60 seconds.
query-max-response-time <*seconds*>	Specifies the maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group <*group-address*>	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface’s IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 7.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
(config)#interface demand 1
(config-demand 1)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 7.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub upstream* on page 663 for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface demand 1
(config-demand 1)#ip mcast-stub downstream
```

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the IGMP proxy. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 8.1	Command was introduced.
Release 11.1	Command was expanded to include the demand interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address>* on page 387, *ip mcast-stub downstream* on page 661, and *ip mcast-stub upstream* on page 663 for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

```
(config)#interface demand 1
(config-demand 1)#ip mcast-stub helper-enable
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 7.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub downstream* on page 661 for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface demand 1
(config-demand 1)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 165,535.
dead-interval <*seconds*>	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range: 0 32,767.
hello-interval <*seconds*>	Specifies the interval between hello packets sent on the interface. Range: 0 32,767.
message-digest-key <*keyid*> **md5** <*key*>	Configures OSPF Message Digest 5 (MD5) authentication (16-byte max) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0 255.
retransmit-interval <*seconds*>	Specifies the time between link-state advertisements (LSAs). Range: 0 32,767.
transmit-delay <*seconds*>	Sets the estimated time required to send an LSA on the interface. Range: 0 32,767.

Default Values

retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second
hello-interval <*seconds*>	10 seconds: Ethernet, point-to-point, Frame Relay, and PPP
dead-interval <*seconds*>	40 seconds

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Example

The following example sets the maximum number of seconds allowed between hello packets to 25,000:

```
(config)#interface demand 1
(config-demand 1)#ip ospf dead-interval 25000
```

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Selects message-digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example specifies that no authentication will be used on the demand interface:

```
(config)#interface demand 1
(config-demand 1)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP and Frame Relay default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface demand 1
(config-demand 1)#ip ospf network broadcast
```

ip policy route-map *<mapname>*

Use the **ip policy route-map** command to associate a route map with a network interface source. Use the **no** form of this command to disable this feature.

Syntax Description

<mapname>	Specifies the route map to associate with this interface.

Default Values

By default, policy-based routing is disabled for all interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example associates the route map named **MyMap** with demand interface **1**:

```
(config)#interface demand 1
(config-demand 1)#ip policy route-map MyMap
```

ip proxy-arp *<address> <subnet mask>*

Use the **ip proxy-arp** to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example, 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy ARP is enabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, the AOS will respond to all proxy ARP requests with its specified MAC address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following example enables proxy ARP on the virtual demand interface:

```
(config)#interface demand 1
(config-demand 1)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

The AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual demand interface to accept only RIP version 2 packets:

```
(config)#interface demand 1
(config-demand 1)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

Use the **ip rip send version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

The AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual demand interface to transmit only RIP version 2 packets:

```
(config)#interface demand 1
(config-demand 1)#ip rip send version 2
```

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> NOTE *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route cache is enabled for all virtual demand interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 2.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

Fast-cache switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast-cache switching on the virtual demand interface:

```
(config)#interface demand 1
(config-demand 1)#ip route-cache
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface (in the format **type slot/port**) that contains the IP address to use as the source address for all packets transmitted on this interface. Type **show ip unnumbered interface ?** for a list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Demand Interface Configuration mode configures the demand interface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, the AOS uses the specified interface information when sending route updates over the unnumbered interface. Static routes may either use the interface name (ppp 1) or the far-end address (if it will be discovered).

Usage Examples

The following example configures the demand interface (labeled **demand 1**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

```
(config)#interface demand 1
(config-demand 1)#ip unnumbered eth 0/1
```

keepalive *<seconds>*

Use the **keepalive** command to enable the transmission of keepalive packets on the interface and specify the time interval in seconds between transmitted packets.

Syntax Description

<seconds>	Defines the time interval (in seconds) between transmitted keepalive packets (valid range: 0 to 32,767 seconds).

Default Values

By default, the time interval between transmitted keepalive packets is 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

If three keepalive packets are sent to an interface with no response, the interface is considered down. To detect interface failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of 5 seconds on the virtual demand interface:

```
(config)#interface demand 1
(config-demand 1)#keepalive 5
```

lldp receive

Use the **lldp receive** command to allow LLDP packets to be received on this interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example configures the demand interface to receive LLDP packets:

```
(config)#interface demand 1
(config-demand 1)#lldp receive
```

lldp send [management-address | port-description | system-capabilities | system-description | system-name | and-receive]

Use the **lldp send** command to configure this interface to transmit LLDP packets or to control the types of information contained in the LLDP packets transmitted by this interface.

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

Be default, all interfaces are configured to transmit and receive LLDP packets of all types.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the demand interface to transmit LLDP packets containing all enabled information types:

```
(config)#interface demand 1
(config-demand 1)#lldp send
```

The following example configures the demand interface to transmit and receive LLDP packets containing all information types:

```
(config)#interface demand 1
(config-demand 1)#lldp send and-receive
```

match-interesting [list *<acl name>* | reverse list *<acl name>*] [in | out]

Use the **match-interesting** command to allow an access list (ACL) to specify which traffic attempting to cross this interface will be considered interesting. Use the **no** form of this command to restore the default values.

Syntax Description

list <*acl name*>	Specifies using an ACL with normal (source, destination) ACL matching logic.
reverse list <*acl name*>	Specifies using an ACL with reverse (destination, source) ACL matching logic.
in	Optional. Specifies that only incoming traffic is interesting.
out	Optional. Specifies that only outgoing traffic is interesting.

Default Values

By default, no interesting traffic is defined.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs demand interface **1** to use the access list **MyACL** when checking for interesting traffic:

```
(config)#interface demand 1
(config-demand 1)#match-interesting list MyACL in
```

mtu *<size>*

Use the **mtu** command to configure the maximum transmit unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:	
	ATM interfaces	64 to 1520
	Demand interfaces	64 to 1520
	Ethernet interfaces	64 to 1500
	FDL interfaces	64 to 256
	HDLC interfaces	64 to 1520
	Loopback interfaces	64 to 1500
	Tunnel interfaces	64 to 18,190
	Virtual Frame Relay sub-interfaces	64 to 1520
	Virtual PPP interfaces	64 to 1500

Default Values

<size>	The default values for the various interfaces are listed below:	
	ATM interfaces	1500
	Demand interfaces	1500
	Ethernet interfaces	1500
	FDL interfaces	256
	HDLC interfaces	1500
	Loopback interfaces	1500
	Tunnel interfaces	1500
	Virtual Frame Relay sub-interfaces	1500
	Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the virtual demand interface:

```
(config)#interface demand 1
(config-demand 1)#mtu 1200
```

peer default ip address *<address>*

Use the **peer default ip address** command to specify the default IP address of the remote end of this interface.

Syntax Description

<address>	Specifies the default IP address for the remote end (A.B.C.D).

Default Values

By default, there is no assigned peer default IP address.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

This command is useful if the peer does not send the IP address option during PPP negotiations.

Usage Examples

The following example sets the default peer IP address to 192.22.71.50:

```
(config)#interface demand 1
(config-demand 1)#peer default ip address 192.22.71.50
```

ppp authentication [chap | eap | pap]

Use the **ppp authentication** command to specify the authentication protocol on the PPP virtual interface that the peer should use to authenticate itself.

Syntax Description

chap	Configures CHAP authentication on the interface.
eap	Configures EAP authentication on the interface.
pap	Configures PAP authentication on the interface.

Default Values

By default, PPP endpoints have no authentication configured.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Technology Review

CHAP and PAP are two authentication methods that enjoy widespread support. Both methods are included in the AOS and are easily configured.

NOTE *The authentication method set up on the local router can be different from that on the peer. Also, just because one router requires authentication from its peer does not mean it also has to authenticate itself to the peer.*

Defining PAP

The Password Authentication Protocol (PAP) is used to verify that the PPP peer is a permitted device by checking a username and password configured on the peer. The username and password are both sent unencrypted across the connecting private circuit.

PAP requires two-way message passing. First, the router that is required to be authenticated (say the peer) sends an authentication request with its username and password to the router requiring authentication (say the local router). The local router then looks up the username and password in the username database within the PPP interface, and if they match sends an authentication acknowledge back to the peer.

> NOTE *The PPP username and password database is separate and distinct from the global username password database. For PAP and CHAP, use the database under the PPP interface configuration.*

Several example scenarios are given below for clarity.

Configuring PAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-demand 1)#ppp authentication pap
Local(config-demand 1)#username farend password same
```

On the peer (hostname Peer):

```
Peer(config-demand 1)#ppp pap sent-username farend password same
```

The first line of the configuration sets the authentication mode as PAP. This means the peer is required to authenticate itself to the local router via PAP. The second line is the username and password expected to be sent from the peer. On the peer, the **ppp pap sent-username** command is used to specify the appropriate matching username and password.

Configuring PAP Example 2: Both routers require the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-demand 1)#ppp authentication pap
Local(config-demand 1)#username farend password far
Local(config-demand 1)#ppp pap sent-username nearend password near
```

On the peer (hostname Peer):

```
Peer(config-demand 1)#ppp authentication pap
Peer(config-demand 1)#username nearend password near
Peer(config-demand 1)#ppp pap sent-username farend password far
```

Now both routers send the authentication request, verify that the username and password sent match what is expected in the database, and send an authentication acknowledge.

Defining CHAP

The Challenge-Handshake Authentication Protocol (CHAP) is a three-way authentication protocol composed of a challenge response and success or failure. The MD5 protocol is used to protect usernames and passwords in the response.

First, the local router (requiring its peer to be authenticated) sends a "challenge" containing only its own unencrypted username to the peer. The peer then looks up the username in the username database within the PPP interface, and if found takes the corresponding password and its own hostname and sends a “response” back to the local router. This data is encrypted. The local router verifies that the username and password are in its own username database within the PPP interface, and if so sends a "success" back to the peer.

NOTE *The PPP username and password database is separate and distinct from the global username password database. For PAP and CHAP, use the database under the PPP interface configuration.*

Several example scenarios are given below for clarity.

Configuring CHAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-demand 1)#ppp authentication chap
Local(config-demand 1)#username Peer password same
```

On the peer (hostname Peer):

```
Peer(config-demand 1)#username Local password same
```

The first line of this configuration sets the authentication mode to CHAP. This means the peer is required to authenticate itself to the local router via CHAP. The second line is the username and password expected to be sent from the peer. The peer must also have the **username** up both to verify the incoming username from the local router and to use the password (along with its hostname) in the response to the local router.

NOTE *Both ends must have identical passwords.*

Configuring CHAP Example 2: Both routers require the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-demand 1)#ppp authentication chap
Local(config-demand 1)#username Peer password same
```

On the peer (hostname Peer):

```
Peer(config-demand 1)#ppp authentication chap
Peer(config-demand 1)#username Local password same
```

This is basically identical to Example 1 except that both routers will now challenge each other and respond.

Configuring CHAP Example 3: Using the ppp chap hostname command as an alternate solution.

On the local router (hostname Local):

```
Local(config-demand 1)#ppp authentication chap
Local(config-demand 1)#username Peer password same
Local(config-demand 1)#ppp chap hostname nearend
```

On the peer (hostname Peer):

```
Peer(config-demand 1)#username nearend password same
```

Notice the peer is expecting username “nearend” even though the local router's hostname is “Local.” Therefore the local router can use the **ppp chap hostname** command to send the correct name on the challenge.

Configuring CHAP Example 4: Using the ppp chap password command as an alternate solution.

On the local router (hostname Local):

```
Local(config-demand 1)#ppp authentication chap
Local(config-demand 1)#username Peer password different
```

On the peer (hostname Peer):

```
Peer(config-demand 1)#username Local password same
Peer(config-demand 1)#ppp chap password different
```

Here the local router challenges with hostname "Local." The peer verifies the name in the username database, but instead of sending the password "same" in the response, it uses the one in the **ppp chap password** command. The local router then verifies that user "Peer" with password "different" is valid and sends a "success."

ppp chap hostname *<hostname>*

Use the **ppp chap hostname** command to configure an alternate hostname for CHAP PPP authentication. Use the **no** form of this command to remove a configured hostname. For more information on PAP and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication [chap | eap | pap]* on page 680.

Syntax Description

<hostname>	Specifies a hostname using an alphanumeric string up to 80 characters in length.

Default Values

By default, there are no configured PPP CHAP hostnames.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example specifies a PPP CHAP hostname of **my_host**:

```
(config)#interface demand 1
(config-demand 1)#ppp chap hostname my_host
```

ppp chap password *<password>*

Use the **ppp chap password** command to configure an alternate password when the peer requires CHAP PPP authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication [chap | eap | pap]* on page 680.

Syntax Description

<password>	Specifies a password using an alphanumeric string up to 80 characters in length.

Default Values

By default, there is no defined PPP CHAP password.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example specifies a PPP CHAP password of **my_password**:

```
(config)#interface demand 1
(config-demand 1)#ppp chap password my_password
```

ppp multilink [fragmentation | interleave]

Use the **ppp multilink** command to enable multilink PPP (MPPP) operation on an existing PPP interface. Use the **no** form of this command to disable.

Syntax Description

fragmentation	Enables multilink fragmentation operation.
interleave	Enables multilink interleave operation.

Default Values

By default, MPPP is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 7.1	Command was introduced.
Release 7.2	Fragmentation and interleave operation were added.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

When enabled, this interface is capable of the following:

- Combining multiple physical links into one logical link.
- Receiving upper layer protocol data units (PDU), fragmenting and transmitting over the physical links.
- Receiving fragments over the physical links and reassembling them into PDUs.

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

The multilink bundle will remain active with a minimum of one physical link. Physical links may be dynamically added or removed from the multilink bundle with minor interruption to traffic flow.

Usage Examples

The following example enables MPPP:

```
(config)#interface demand 1
(config-demand 1)#ppp multilink
```

ppp pap sent-username *<username>* password *<password>*

Use the **ppp pap sent-username/password** command to configure a username and password when the peer requires PAP PPP authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication [chap | eap | pap]* on page 680.

Syntax Description

<username>	Specifies a username by alphanumeric string up to 80 characters in length (the username is case-sensitive).
<password>	Specifies a password by alphanumeric string up to 80 characters in length (the password is case-sensitive).

Default Values

By default, there is no defined **ppp pap sent-username** and **password**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example specifies a PPP PAP sent-username of **local** and a password of **my_password**:

```
(config)#interface demand 1
(config-demand 1)#ppp pap sent-username local password my_password
```

qos-policy out *<mapname>*

Use the **qos-policy out** command to apply a previously-configured QoS map to an interface. Use the **no** form of this command to remove the map from the interface. The keyword **out** specifies that this policy will be applied to outgoing packets.

Syntax Description

<mapname>	Specifies the name of a previously-created QoS map (refer to *qos map <mapname> <sequence number>* on page 434 for more information).

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 6.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the demand 1 interface:

```
(config)#interface demand 1
(config-demand 1)#qos-policy out VOICEMAP
```

resource pool *<pool name>*

Use the **resource pool** command to associate a resource pool with the demand interface. No more than one resource pool may be associated with an interface. Refer to *resource pool-member <pool-name> [<cost>]* on page 693 for more information. Use the **no** form of this command to restore the default values.

Syntax Description

<pool name>	Specifies the resource pool that this interface will use to originate/answer demand connections.

Default Values

By default, no resource pool is associated with this interface.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example associates the resource pool named **Pool1** with demand interface **1**:

```
(config)#interface demand 1
(config-demand 1)#resource pool Pool1
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the virtual demand interface:

```
(config)#interface demand 1
(config-demand 1)#no snmp trap link-status
```

username *<username>* **password** *<password>*

Configures the username and password of the peer to use for demand authentication.

Syntax Description

<username>	Specifies a username by alphanumerical string up to 30 characters in length (the username is case-sensitive).
<password>	Specifies a password by alphanumerical string up to 30 characters in length (the password is case-sensitive).

Default Values

By default, there is no established username and password.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command expanded to include the demand interface.

Functional Notes

PAP uses this entry to check received information from the peer. CHAP uses this entry to check the received peer hostname and a common password.

Usage Examples

The following example creates a username of **ADTRAN** with password **ADTRAN** for the demand link labeled **5**:

```
(config)#interface demand 5
(config-demand 5)#username ADTRAN password ADTRAN
```

FRAME RELAY INTERFACE CONFIG COMMAND SET

To activate the Frame Relay Interface Configuration mode, enter the **interface frame-relay** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface frame-relay 1
(config-fr 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

bandwidth <value> on page 693

encapsulation frame-relay ietf on page 694

fair-queue <threshold> on page 695

frame-relay commands begin on page 696

hold-queue <queue size> out on page 708

max-reserved-bandwidth <percent> on page 709

qos-policy out <mapname> on page 710

snmp trap on page 712

snmp trap link-status on page 713

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies bandwidth in kbps.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the Frame Relay interface to 10 Mbps:

```
(config)#interface frame-relay 1
(config-fr 1)#bandwidth 10000
```

encapsulation frame-relay ietf

Use the **encapsulation frame-relay ietf** command to configure the encapsulation on a virtual Frame Relay interface as IETF (RFC1490). Currently, this is the only encapsulation setting. Settings for this option must match the far-end router's settings in order for the Frame Relay interface to become active.

Syntax Description

No subcommands.

Default Values

By default, all Frame Relay interfaces use IETF encapsulation.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the endpoint for IETF encapsulation:

```
(config)#interface frame-relay 1
(config-fr 1)#encapsulation frame-relay ietf
```

fair-queue *<threshold>*

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable first-in-first-out (FIFO) queueing for an interface. WFQ is enabled by default for WAN interfaces.

Syntax Description

<threshold>	Optional. Specifies the maximum number of packets that can be present in each conversation sub-queue. Packets received for a conversation after this limit is reached are discarded. Range: 16 to 512.

Default Values

By default, **fair-queue** is enabled with a threshold of 64 packets.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

```
(config)#interface frame-relay 1
(config-fr 1)#fair-queue 100
```

frame-relay intf-type [dce | dte | nni]

Use the **frame-relay intf-type** command to define the Frame Relay signaling role needed for the endpoint. Use the **no** form of this command to return to the default value.

Syntax Description

dce	Specifies DCE or network-signaling role. Use this interface type when you need the unit to emulate the frame switch.
dte	Specifies DTE or user-signaling role. Use this interface type when connecting to a Frame Relay switch (or piece of equipment emulating a frame switch).
nni	Configures the interface to support both network and user signaling (DTE or DCE) when necessary.

Default Values

By default, **frame-relay intf-type** is set to **dte**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the Frame Relay endpoint for DCE signaling:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay intf-type dce
```

frame-relay lmi-n391dce *<polls>*

Use the **frame-relay lmi-n391dce** command to set the N391 full status polling counter for the DCE endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<polls>	Sets the counter value (valid range: 1 to 255).

Default Values

By default, the polling counter for the DCE endpoint is set to six polls.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The N391 counter determines how many link integrity polls occur in between full status polls. The number of link integrity polls between full status polls is n - 1, where n represents the full status poll. n can be set to any number between 1 and 255, but the default is used for most applications.

Usage Examples

The following example sets the N391 counter for three polls:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-n391dce 3
```

frame-relay lmi-n391dte *<polls>*

Use the **frame-relay lmi-n391dte** command to set the N391 full status polling counter for the DTE endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<polls>	Sets the counter value (valid range: 1 to 255).

Default Values

By default, the polling counter for the DTE endpoint is set to six polls.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The N391 counter determines how many link integrity polls occur in between full status polls. The number of link integrity polls between full status polls is n - 1, where n represents the full status poll. n can be set to any number between 1 and 255, but the default is used for most applications.

Usage Examples

The following example sets the N391 counter for three polls:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-n391dte 3
```

frame-relay lmi-n392dce *<threshold>*

Use the **frame-relay lmi-n392dce** command to set the N392 error threshold for the DCE endpoint. Typical applications should leave the default value for this setting. Use the **no** form of this command to return to the default value.

Syntax Description

<threshold>	Sets the threshold value (valid range: 1 to 10).

Default Values

By default, the error threshold for the DCE endpoint is set to three errors.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

If the error threshold is met, the signaling state status is changed to down, indicating a service-affecting condition. This condition is cleared once N393 consecutive error-free events are received. N392 defines the number of errors required in a given event window, while N393 defines the number of polling events in each window.

For example:

If N392 = and N393 = 4, then if three errors occur within any four events, the interface is determined inactive.

Usage Examples

The following example sets the N392 threshold for 5 seconds:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-n392dce 5
```

frame-relay lmi-n392dte *<threshold>*

Use the **frame-relay lmi-n392dte** command to set the N392 error threshold for the DTE endpoint. Typical applications should leave the default value for this setting. Use the **no** form of this command to return to the default value.

Syntax Description

<threshold>	Sets the threshold value (valid range: 1 to 10).

Default Values

By default, the error threshold for the DTE endpoint is set to three errors.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

If the error threshold is met, the signaling state status is changed to down, indicating a service-affecting condition. This condition is cleared once N393 consecutive error-free events are received. N392 defines the number of errors required in a given event window, while N393 defines the number of polling events in each window.

For example:

If N392 = 3 and N393 = 4, then if three errors occur within any four events, the interface is determined inactive.

Usage Examples

The following example sets the N392 threshold for five errors:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-n392dte 5
```

frame-relay lmi-n393dce *<counter>*

Use the **frame-relay lmi-n393dce** to set the N393 LMI monitored event counter for the DCE endpoint. Typical applications should leave the default value for this counter. Use the **no** form of this command to return to the default value.

Syntax Description

<counter>	Sets the counter value (valid range: 1 to 10).

Default Values

By default, the LMI monitored event counter for the DCE endpoint is set to four events.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sets the N393 threshold for five events:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-n393dce 5
```

frame-relay lmi-n393dte *<counter>*

Use the **frame-relay lmi-n393dte** command to set the N393 LMI monitored event counter for the DTE endpoint. Typical applications should leave the default value for this counter. Use the **no** form of this command to return to the default value.

Syntax Description

<*counter*>	Sets the counter value (valid range: 1 to 10).

Default Values

By default, the LMI monitored event counter for the DTE endpoint is set to four events.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example sets the N393 threshold for five events:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-n393dte 5
```

frame-relay lmi-t391dte *<seconds>*

Use the **frame-relay lmi-t391dte** command to set the T391 signal polling timer for the DTE endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<seconds>	Sets the timer value in seconds (valid range: 5 to 30).

Default Values

By default, the signal polling timer for the DTE endpoint is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The T391 timer sets the time (in seconds) between polls to the Frame Relay network.

Usage Examples

The following example sets the T391 timer for 15 seconds:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-t391dte 15
```

frame-relay lmi-t392dce *<seconds>*

Use the **frame-relay lmi-t392dce** command to set the T392 polling verification timer for the DCE endpoint. Typical applications should leave the default value for this timer. Use the **no** form of this command to return to the default value.

Syntax Description

<seconds>	Sets the timer value in seconds (valid range: 5 to 30).

Default Values

By default, the polling verification timer for the DCE endpoint is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The T392 sets the timeout (in seconds) between polling intervals. This parameter needs to be a few seconds longer than the T391 setting of the attached Frame Relay device.

Usage Examples

The following example sets the T392 timer for 15 seconds:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-t392dce 15
```

frame-relay lmi-type [ansi | auto | cisco | none | q933a]

Use the **frame-relay lmi-type** command to define the Frame Relay signaling (LMI) type. Use the **no** form of the command to return to the default value.

Syntax Description

ansi	Specifies Annex D signaling method.
auto	Automatically determines signaling type by messages received on the frame circuit.
cisco	Specifies Group of 4 signaling method.
none	Turns off signaling on the endpoint. This is used for dial-backup connections to ADTRAN IQ and Express series products.
q933a	Specifies Annex A signaling method.

Default Values

By default, the Frame Relay signaling type is set to **ansi**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 2.1	Added signaling type **none** to provide support for dial-backup to ADTRAN IQ and Express series products.

.

Usage Examples

The following example sets the signaling method for the endpoint to **cisco**:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay lmi-type cisco
```

frame-relay multilink [ack *<seconds>* | bandwidth-class *<class>* *<threshold>* | hello *<seconds>* | retry *<number>*]

Use the **frame-relay multilink** command to enable the Frame Relay multilink interface. When the **no** form of this command is issued, all configuration options associated with this command and cross-connects made to this interface are removed.

Syntax Description

ack *<seconds>*	Optional. Specifies a wait for acknowledgement time (in seconds) for every bundle link in the bundle. Range: 1 to 180 seconds.	
bandwidth-class	Optional. Specifies the class of operation, placing a minimum limit on the acceptable amount of bandwidth required for a bundle to up.	
<class>	Optional. Specifies the class of operation. Range is A to C:	
	Class A	A single active link is sufficient for the bundle to be up.
	Class B	All defined bundle links must be active for the bundle to be up.
	Class C	A minimum threshold of links must be active for the bundle to be up.
<threshold>	Optional. Specifies the minimum number of active bundle links required for a class C bundle to be in the up state. This option will not be available unless Class C is specified. Range: 1 to 65,535 links.	
hello *<seconds>*	Optional. Specifies the time (in seconds) between hello messages for every bundle link in the bundle. Range: 1 to 180 seconds.	
retry *<number>*	Optional. Specifies the number of times a bundle link will retransmit a message while waiting for acknowledgement. Range: 1 to 5 times.	

Default Values

The default **ack** value is 4 seconds. The default **hello** value is 10 seconds. The default *<class>* value is a. The default **retry** value is 2.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Note

This command is different from **ppp multilink**. In **ppp multilink**, if multiple cross-connects are configured for the PPP interface without multilink PPP being enabled, the first link to bring up LCP will be the only link actually cross-connected. In Frame Relay multilink, since there is no protocol corresponding to LCP, all cross-connects will be removed and the user will be free to re-issue any cross-connect.

Usage Examples

The following example enables the Frame Relay multilink interface and sets the time between **hello** messages to 45 seconds:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay multilink hello 45
```

The following example specifies Class B operation:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay multilink bandwidth-class b
```

The following example specifies Class C operation with a threshold of 5:

```
(config)#interface frame-relay 1
(config-fr 1)#frame-relay multilink bandwidth-class c 5
```

hold-queue *<queue size>* out

Use the **hold-queue out** command to change the overall size of an interface's WAN output queue.

Syntax Description

<queue size>	Specifies the total number of packets the output queue can contain before packets are dropped. Range: 16 to 1000.

Default Values

The default queue size for WFQ is 400. The default queue size for PPP FIFO and Frame Relay round robin is 200.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the overall output queue size to 700:

```
(config)#interface frame-relay 1
(config-fr 1)#hold-queue 700 out
```

max-reserved-bandwidth *<percent>*

Use the **max-reserved-bandwidth** command to define the maximum amount of interface bandwidth reserved for Quality of Service (QoS). Use the **no** form of this command to return to the default value.

Syntax Description

<percent>	Specifies the maximum amount of bandwidth to reserve for QoS. This setting is configured as a percentage of the total interface speed. Range: 1 to 100 percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the reserved bandwidth maximum at 80 percent:

```
(config)#interface frame-relay 1
(config-fr 1)#max-reserved-bandwidth 80
```

qos-policy out *<mapname>*

Use the **qos-policy out** command to apply a previously-configured QoS map to an interface. Use the **no** form of this command to remove the map from the interface. The **out** keyword specifies that this policy will be applied to outgoing packets.

Syntax Description

<mapname>	Specifies the name of a previously-created QoS map (refer to *qos map <mapname> <sequence number>* on page 434 for more information).

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross-connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when ADSL finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the Frame Relay interface:

```
(config)#interface frame-relay 1
(config-fr 1)#qos-policy out VOICEMAP
```

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and sub-interfaces) have SNMP traps enabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Ethernet sub-interfaces and Gigabit Ethernet interfaces.

Usage Examples

The following example enables SNMP on the virtual Frame Relay interface:

```
(config)#interface frame-relay 1
(config-fr 1)#snmp trap
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the Frame Relay interface:

```
(config)#interface frame-relay 1
(config-fr 1)#no snmp trap link-status
```

FRAME RELAY SUB-INTERFACE CONFIG COMMAND SET

To activate the Frame Relay Sub-Interface Configuration mode, enter the **interface frame-relay** command (and specify a sub-interface) at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface frame-relay 1.16
(config-fr 1.16)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

description <text> on page 31

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 715

bandwidth <value> on page 718

bridge-group <group#> on page 719

crypto map <mapname> on page 720

dial-backup commands begin on page 722

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 738

frame-relay commands begin on page 740

ip commands begin on page 744

lldp receive on page 772

lldp send [management-address l port-description l system-capabilities l system-description l system-name l and-receive] on page 773

mtu <size> on page 775

spanning-tree commands begin on page 776

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic on an interface. Use the **no** form of this command to remove an access policy association.

> NOTE *Configured access policies will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<*policyname*>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 6.1	Command was expanded to 1000 and 2000 Series units.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access-policy** <*policy name*>.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the Frame Relay sub-interface labeled 1.16:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:

(config)#**ip policy-class UnTrusted**
(config-policy-class)#**allow list InWeb**

Associate the access list with the Frame Relay sub-interface labeled 1:

(config)#**interface frame-relay 1.16**
(config-fr 1.16)#**access-policy UnTrusted**

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:

Enable the security features of the AOS using the **ip firewall** command.

Step 2:

Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** *<A.B.C.D>* to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the *<A.B.C.D> <wildcard>* format to match all IP addresses in a "range." Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a "don't care." For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:

Create an access policy that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list *<access list names>*

All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list *<access list names>*

All packets passed by the access list(s) entered will be dropped from the router system.

allow list *<access list names>* **policy** *<access policy name>*

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the Frame Relay sub-interface labeled 1:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#access-policy MatchAll
```

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies bandwidth in kbps.

Default Values

To view default values use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the Frame Relay interface to 10 Mbps:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#bandwidth 10000
```

bridge-group *<group#>*

Use the **bridge-group** command to assign an interface to the specified bridge group. This command is supported on all Ethernet interfaces, PPP virtual interfaces, and Frame Relay virtual sub-interfaces. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<group#>	Specifies the bridge group number (1 to 255).

Default Values

By default, there are no configured bridge groups.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1 bridge, Ethernet to Frame Relay sub-interface).

Usage Examples

The following example assigns the Frame Relay sub-interface labeled 1.16 to bridge group 1:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#bridge-group 1
```

crypto map *<mapname>*

Use the **crypto map** command to associate crypto maps with the interface.

> *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

<mapname>	Specifies the crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

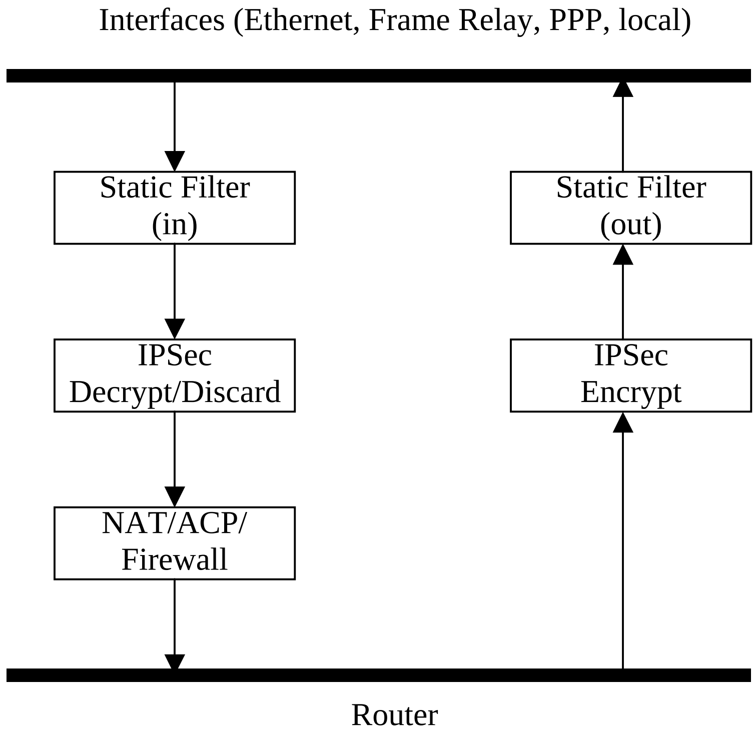
Command History

Release 4.1	Command was introduced.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following notes in mind.

When defining the policy-class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the Frame Relay interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#crypto map MyMap
```

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the Frame Relay sub-interface to automatically attempt a dial-backup upon failure. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial-backup upon a failure.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables automatic dial-backup on the endpoint:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup auto-backup
```

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial-backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to automatically restore the primary connection when the failure condition clears:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup auto-restore
```

dial-backup backup-delay *<seconds>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<seconds>	Specifies the delay period (in seconds) a failure must be active before the AOS will enter backup operation on the interface. Range: 10 to 86,400 seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to wait 60 seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup backup-delay 60
```

dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]

Use the **dial-backup call-mode** command to combine user data with pattern data to ensure data does not mirror standard DDS loop codes (use only on 64 kbps circuits without Frame Relay signaling). Use the **no** form of this command to return to the default value.

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer.**

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The majority of the configuration for Frame Relay dial-backup is configured in the Frame Relay sub-interface. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname "Remote3200"
enable password adtran
!
interface eth 0/1
  ip address  192.168.1.254  255.255.255.0
  no shutdown
!
interface modem 1/3
 no shutdown
!
```

```
interface t1 1/1
  coding b8zs
  framing esf
  clock source line
  tdm-group 1 timeslots 1-24
  no shutdown
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  cross-connect 1 t1 1/1 1 fr 1
!
interface fr 1.16 point-to-point
  frame-relay interface-dlci 16
  ip address 10.1.1.2 255.255.255.252
  dial-backup call-mode originate
  dial-backup number 5551111 analog
  dial-backup number 5552222 analog
!
ip route 0.0.0.0  0.0.0.0  10.1.1.1
!
line telnet 0 4
  password adtran
```

Sample config for central router (dialing in)

```
hostname "Central3200"
enable password adtran
!
interface eth 0/1
  ip address  192.168.100.254  255.255.255.0
  no shutdown
!
interface modem 1/3
 no shutdown
!
interface t1 1/1
  coding b8zs
  framing esf
  clock source line
  tdm-group 1 timeslots 1-24
  no shutdown
!
interface fr 1 point-to-point
  frame-relay lmi-type ansi
  no shutdown
  cross-connect 1 t1 1/1 1 fr 1
```

```
!
interface fr 1.100 point-to-point
  frame-relay interface-dlci 100
  ip address 10.1.1.1 255.255.255.252
  dial-backup call-mode answer
  dial-backup number 555-8888 analog
!
line telnet 0 4
  password adtran
```

Usage Examples

The following example configures the AOS to answer dial-backup calls on this endpoint but never generate calls:

(config)#**interface frame-relay 1.16**
(config-fr 1.16)#**dial-backup call-mode answer-always**

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial-backup, where in the configuration the AOS accesses specific routing information, etc.):

Dialing Out

1. The AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, the AOS matches the number dialed to a Frame Relay sub-interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number <digits> [analog | digital-56k | digital 64k] <isdn min chan> <isdn max chan> <interface>* on page 731).
3. When placing the call, the AOS uses the configuration of the related Frame Relay sub-interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, the AOS places a call to the second number if configured. The second number to be dialed references a separate Frame Relay sub-interface.

Dialing In

1. The AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured Frame Relay sub-interface.
3. If a match is found, the call connects and the AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from Caller ID, the call is terminated.

dial-backup connect-timeout *<seconds>*

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<seconds>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call (valid range: 10 to 300).

Default Values

By default, the **dial-backup connect-timeout** period is set to 60 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to wait 120 seconds before retrying a failed dial-backup call:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup connect-timeout 120
```

dial-backup force [backup | primary]

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

backup	Force backup regardless of primary link state.
primary	Force primary link regardless of its state.

Default Values

By default, this feature is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to force this interface into dial-backup:

```
(config)#interface frame-relay 1.16
(config-fr 1.161)#dial-backup force backup
```

dial-backup maximum-retry *<attempts>*

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<attempts>	Selects the number of call retries that will be made after a link failure (valid range: 0 to 15). Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to 0 attempts.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to retry a dial-backup call four times before considering backup operation not available:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup maximum-retry 4
```

dial-backup number *<digits>* [analog | digital-56k | digital 64k] *<isdn min chan> <isdn max chan> <interface>*

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<digits>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates number connects to an analog modem.
digital-56k	Indicates number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates number belongs to a digital 64 kbps per DS0 connection.
<isdn min chan>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection (Range: 1 to 24).
<isdn max chan>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection (Range: 1 to 24).
<interface>	Specifies the Frame Relay sub-interface (e.g., **fr 3.1**) to use when originating or answering using this number.

Default Values

By default, there are no configured dial-backup numbers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to dial 704-555-1212 (digital 64 kbps connection) to initiate dial-backup operation on this endpoint using sub-interface Frame Relay 3.1:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup number 7045551212 digital-64k 1 1 fr 3.1
```

dial-backup priority *<value>*

Use the **dial-backup priority** command to select the backup priority for this interface. This command allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<value>	Sets the relative priority of this link (valid range: 0 to 100). A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to 50.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example assigns the highest priority to this endpoint:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup priority 100
```

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer* | *answer-always* | *originate* | *originate-answer* | *originate-answer-always]* on page 725.

Syntax Description

No subcommands.

Default Values

By default, the AOS does not randomize the dial-backup call timers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to randomize the dial-backup timers associated with this endpoint:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup randomize-timers
```

dial-backup redial-delay *<seconds>*

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<seconds>	Specifies the delay in seconds between attempting to re-dial a failed backup attempt. Range: 10 to 3600.

Default Values

By default, **dial-backup redial-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures a redial delay of 25 seconds on this endpoint:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup redial-delay 25
```

dial-backup restore-delay *<seconds>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is "bouncing" in and out of alarm. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

<seconds>	Specifies the number of seconds the AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range: 10 to 86,400.

Default Values

By default, **dial-backup restore-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures the AOS to wait 30 seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup restore-delay 30
```

dial-backup schedule [day | enable-time | disable-time]

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial-backup (as specified). For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

day	Sets the days to allow backup (valid range: Monday through Sunday).
enable-time	Sets the time of day to enable backup. Time is entered in 24-hour format (00:00).
disable-time	Sets the time of day to disable backup.

Default Values

By default, dial-backup is enabled for all days and times if the dial-backup auto-backup command has been issued and the dial-backup schedule has not been entered.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables dial-backup Monday through Friday 8:00 am to 7:00 pm:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup schedule enable-time 08:00
(config-fr 1.16)#dial-backup schedule disable-time 19:00
(config-fr 1.16)#no dial-backup schedule day Saturday
(config-fr 1.16)#no dial-backup schedule day Sunday
```

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on Frame Relay dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 725.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example deactivates the configured dial-backup interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dial-backup shutdown
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

Refer to *Functional Notes* below for argument descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A web-based interface provides two levels of control over your domain, catering to average or power users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service, in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address doesn't change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name) Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com) you need Custom DNS service which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the Dynamic DNS to **dyndns-custom** with hostname **host**, username **user**, and password **pass**:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#dynamic-dns dyndns-custom host user pass
```

frame-relay bc *<committed burst value>*

Use the **frame-relay bc** command to set the b_c (committed burst) value for a Frame Relay sublink. The value is in bits. Use the **no** form of this command to return to default.

Syntax Description

<committed burst value>	Specifies the committed burst value (in bits) for the sublink.

Default Values

By default, the committed burst value is set to 0 (no limit).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

The time interval is always one second, so this can also be considered bits per second. Shaping is performed on a sliding one-second window to make maximum use of configured bandwidth. Note that when both b_c and b_e are non-zero, shaping is performed on the virtual circuit. The circuit is limited to the sum of b_c and b_e , and it is recommended that the sum always be greater than 8000.

Usage Examples

The following example configures the Frame Relay sublink with a committed burst value of 128,000 bits:

```
(config)#interface frame-relay 1.1
(config-fr 1.16)#frame-relay bc 128000
```

frame-relay be *<excessive burst value>*

Use the **frame-relay be** command to set the b_e (excessive burst) value for a Frame Relay sublink. The value is in bits. Use the **no** form of this command to return to default.

Syntax Description

<excessive burst value>	Specifies the excessive burst value (in bits) for the sublink.

Default Values

By default, the excessive burst value is set to 0 (no limit).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

The time interval is always one second, so this can also be considered bits per second. Shaping is performed on a sliding one-second window to make maximum use of configured bandwidth. Note that when both b_c and b_e are non-zero, shaping is performed on the virtual circuit. The circuit is limited to the sum of b_c and b_e , and it is recommended that the sum always be greater than 8000.

Usage Examples

The following example configures the Frame Relay sublink with an excessive burst value of 64,000 bits:

```
(config)#interface frame-relay 1.1
(config-fr 1.16)#frame-relay be 64000
```

frame-relay fragment *<threshold>*

Use the **frame-relay fragment** command to set the FRF.12 fragmentation threshold. Use the **no** form of this command to erase the configured threshold.

Syntax Description

<threshold>	Specifies the fragmentation threshold. Valid fragmentation thresholds are greater than or equal to 64 and less than or equal to 1600.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

For Frame Relay fragmentation to take effect, rate-limiting must be enabled by setting the committed burst rate and excessive burst rate. Refer to *frame-relay bc <committed burst value>* on page 740 and *frame-relay be <excessive burst value>* on page 741 for more information.

Usage Examples

The following example enables FRF.12 fragmentation on a sublink:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#frame-relay bc 64000
(config-fr 1.16)#frame-relay be 16
(config-fr 1.16)#frame-relay fragmentation 100
```

The following example disables FRF.12 fragmentation on a sublink:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#no frame-relay fragment
```

frame-relay interface-dlci *<dlci>*

Use the **frame-relay interface-dlci** command to configure the Data Link Connection Identifier (DLCI) for the Frame Relay sub-interface. This setting should match the DLCI supplied by your Frame Relay service provider. Use the **no** form of this command to remove the configured DLCI.

Syntax Description

<dlci>	Specifies numeric value supplied by your provider.

Default Values

By default, the DLCI is populated with the sub-interface identifier. For example, if configuring the virtual Frame Relay sub-interface labeled **fr 1.20**, the default DLCI is **20**.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example configures a DLCI of 72 for this Frame Relay endpoint:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#frame-relay interface-dlci 72
```

ip access-group *<listname>* [in | out]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Specifies the IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into the Frame Relay sub-interface:

```
(config)#interface frame-relay 1.16
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#int frame-relay 1.16
(config-fr 1.16)#ip access-group TelnetOnly in
```

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface.

ip address dhcp [client-id [<*interface*> **|** <*identifier*>**] hostname** <*"string"*>**]**

Syntax Description

client-id	Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.
<*interface*>	Specifies an interface, thus defining the client identifier as the hexadecimal MAC address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type). For example, specifying the **client-id ethernet 0/1** (where the Ethernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet). Refer to *hardware-address <hardware-address> <type>* on page 1152 for a detailed listing of media types.
<*identifier*>	Specifies a custom client-identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters). For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the <*identifier*> option.
host name	Optional. Specifies a text string (to override the global router name) to use as the name in the DHCP option 12 field.
<*"string"*>	String (encased in quotation marks) of up to 35 characters to use as the name of the host for DHCP operation.
no-default-route	Specifies that the AOS not install the default route obtained via DHCP.
no-domain-name	Specifies that the AOS not install the domain name obtained via DHCP.
no-nameservers	Specifies that the AOS not install the DNS servers obtained via DHCP.

Default Values

client-id	Optional. By default, the client identifier is populated using the following formula: TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address <hardware-address> <type>* on page 1152 for a detailed listing of media types), and the MAC ADDRESS is the Media Access Control (MAC) address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field).

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT#: Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:

8	7	6	5	4	3	2	1
DLCI (high order)						C/R	EA
DLCI (lower)				FECN	BECN	DE	EA

Where the FECN, BECN, C/R, DE, and high order extended address (EA) bits are assumed to be 0 and the lower order EA bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 address:
DLCI (decimal) / Q.922 address (hex)
16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

hostname Optional. By default, the host name is the name configured using the Global Configuration **hostname** command.

<“string”> By default, the host name is the name configured using the Global Configuration **hostname** command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1 Command was introduced.

Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many Internet Service Providers (ISPs) require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

Usage Examples

The following example enables DHCP operation on the virtual Frame Relay interface (labeled 1.16):

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip address dhcp
```

ip address *<address>* *<mask>* secondary

Use the **ip address** command to define an IP address on the specified interface. Use the optional **secondary** keyword to define a secondary IP address. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<mask>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Keyword used to configure a secondary IP address for the specified interface.

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use secondary IP addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IP addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IP addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IP address of **192.22.72.101/30**:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip address 192.22.72.101 255.255.255.252 secondary
```

ip dhcp [release | renew]

Use the **ip dhcp** command to release or renew the DHCP IP address. This command is only applicable when using DHCP for IP address assignment.

Syntax Description

release	Releases DHCP IP address.
renew	Renews DHCP IP address.

Default Values

No default values required for this command.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example releases the IP DHCP address for the virtual interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip dhcp release
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure the AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <port number>* on page 378 *for more information.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets.

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper-address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address **192.33.5.99**:

```
(config)#interface frame-relay 1.16
(config)#ip forward-protocol udp domain
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description

immediate-leave	If only one host (or IGMP snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval <*milliseconds*>	Controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65535 ms. Default: 1000 ms.
querier-timeout <*seconds*>	Specifies the number of seconds that the router waits after the current querier’s last query before it takes over as querier (IGMP V2). Range: 60 to 300 seconds. Default: 2x the **query-interval** value.
query-interval <*seconds* >	Specifies the interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65,535 seconds. Default: 60 seconds.
query-max-response-time <*seconds*>	Specifies the maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group <*group-address*>	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface’s IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding. Refer to *ip mcast-stub helper-address <ip address>* on page 387 and y for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip mcast-stub downstream
```

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the IGMP proxy. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include Frame Relay sub-interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address>* on page 387, *ip mcast-stub downstream* on page 754, and *ip mcast-stub upstream* on page 756 for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

```
(config)#interface frame relay 1.16
(config-fr 1.16)#ip mcast-stub helper-enable
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. Refer to *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub downstream* on page 754 for more information.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key <*password*>	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost <*value*>	Specifies he OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 165,535.
dead-interval <*seconds*>	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range: 0 to 32,767.
hello-interval <*seconds*>	Specifies the interval between hello packets sent on the interface. Range: 0 to 32,767.
message-digest-key <*keyid*> **md5** <*key*>	Configures OSPF Message Digest 5 (MD5) authentication (16-byte maximum) keys.
priority <*value*>	Sets the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0-255.
retransmit-interval <*seconds*>	Specifies the time between link-state advertisements (LSAs). Range: 0 to 32,767.
transmit-delay <*seconds*>	Sets the estimated time required to send an LSA on the interface. Range: 0 to 32,767.

Default Values

retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second
hello-interval <*seconds*>	10 seconds: Ethernet, point-to-point, Frame Relay, and PPP
dead-interval <*seconds*>	40 seconds

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Selects message-digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, this is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example specifies that no authentication will be used on the Frame Relay interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP and Frame Relay default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip ospf network broadcast
```

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM Sparse Mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip pim sparse-mode
```

ip pim-sparse dr-priority *<priority number>*

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the routers priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<priority number>	Specifies the priority number for the DR router. Valid range is 1 to 4,294,967,295.

Default Values

By default, the DR priority is set to 1.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the DR priority to 5:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip pim-sparse dr-priority 5
```

ip pim-sparse hello-timer *<time>*

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time in seconds between hello transmissions. Valid range is 10 to 12,600 seconds.

Default Values

By default, the hello timer is set to 30 seconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the hello timer to 60 seconds:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip pim-sparse hello-timer 60
```

ip pim-sparse nbr-timeout *<time>*

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is 30 to 10,800 seconds.

Default Values

By default, the nbr-timeout is set to 105 seconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip pim-sparse nbr-timeout 300
```

ip pim-sparse override-interval *<time>*

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the LAN may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the delay time in milliseconds. Valid range is 0 to 65,535 milliseconds.

Default Values

By default, the override-interval is set to 2500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override-interval to 3000 milliseconds:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip pim-sparse override-interval 3000
```

ip pim-sparse propagation-delay *<time>*

Use the **ip pim-sparse propagation-delay** command to specify protocol-independent multicast (PIM) sparse join/prune propagation delay. This is the expected propagation delay in milliseconds over the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the expected propagation delay in milliseconds. Valid range is 0 to 32,767 milliseconds.

Default Values

By default, the propagation-delay is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation-delay to 1000 milliseconds:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip pim-sparse propagation-delay 1000
```

ip policy route-map *<policy name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<policy name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip policy route-map policy1
```

ip proxy-arp *<address> <subnet mask>*

Use the **ip proxy-arp** to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy ARP is enabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, the AOS will respond to all proxy ARP requests with its specified MAC address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following enables proxy ARP on the Frame Relay sub-interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that will override the **version** (in the Router RIP) configuration.

The AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures a Frame Relay sub-interface to accept only RIP version 2 packets:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** to specify a RIP version that will override the **version** (in the Router RIP) configuration.

The AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures a Frame Relay sub-interface to transmit only RIP version 2 packets:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip rip send version 2
```

ip route-cache *<address>*

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> NOTE *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route cache is enabled for all virtual PPP interfaces.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast-cache switching on a Frame Relay sub-interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip route-cache
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface (in the format **type slot/port**) that contains the IP address to use as the source address for all packets transmitted on this interface.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include demand interfaces.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Frame Relay Sub-Interface Configuration mode configures the Frame Relay sub-interface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, the AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the Frame Relay interface (labeled **frame-relay 1.16**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#ip unnumbered eth 0/1
```

lldp receive

Use the **lldp receive** command to allow LLDP packets to be received on this interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the Frame Relay sub-interface to receive LLDP packets:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#lldp receive
```

lldp send [management-address | port-description | system-capabilities | system-description | system-name | and-receive]

Use the **lldp send** command to configure this interface to transmit LLDP packets or to control the types of information contained in the LLDP packets transmitted by this interface.

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device’s system capabilities on this interface.
system-description	Enables transmission of this device’s system description on this interface.
system-name	Enables transmission of this device’s system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

Be default, all interfaces are configured to transmit and receive LLDP packets of all types.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the Frame Relay sub-interface to transmit LLDP packets containing all enabled information types:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#lldp send
```

The following example configures the Frame Relay sub-interface to transmit and receive LLDP packets containing all information types:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#lldp send and-receive
```

mtu *<size>*

Use the **mtu** command to configure the maximum transmit unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size> Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:

ATM interfaces	64 to 1520
Demand interfaces	64 to 1520
Ethernet interfaces	64 to 1500
FDL interfaces	64 to 256
HDLC interfaces	64 to 1520
Loopback interfaces	64 to 1500
Tunnel interfaces	64 to 18,190
Virtual Frame Relay sub-interfaces	64 to 1520
Virtual PPP interfaces	64 to 1500

Default Values

<size> The default values for the various interfaces are listed below:

ATM interfaces	1500
Demand interfaces	1500
Ethernet interfaces	1500
FDL interfaces	256
HDLC interfaces	1500
Loopback interfaces	1500
Tunnel interfaces	1500
Virtual Frame Relay sub-interfaces	1500
Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the Frame Relay interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#mtu 1200
```

spanning-tree bpdufilter [enable | disable]

Use the **spanning-tree bpdufilter** command to block BPDUs from being transmitted and received on this interface. To return to the default value, use the **no** form of this command.

Syntax Description

enable	Enables the BPDU filter.
disable	Disables the BPDU filter.

Default Values

By default, this command is set to disable.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The purpose of this command is to remove a port from participation in the spanning tree. This might be beneficial while debugging a network setup. It normally should not be used in a live network.

Usage Examples

The following example enables the BPDU filter on the interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree bpdufilter enable
```

spanning-tree bpduguard [enable | disable]

Use the **spanning-tree bpduguard** command to block BPDUs from being received on this interface. To return to the default value, use the **no** form of this command.

Syntax Description

enable	Enables the BPDU block.
disable	Disables the BPDU block.

Default Values

By default, this command is set to disable.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables the BPDU guard on the interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree bpduguard enable
```

spanning-tree edgeport

Use the **spanning-tree edgeport** command to set this interface to be an edgeport. This command overrides the Global setting (refer to *spanning-tree edgeport default* on page 459). Use the **no** form of this command to return to the default value.

Syntax Description

No subcommands.

Default Values

By default, this command is set to disable.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures the interface to be an edgeport:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree edgeport
```

An individual interface can be configured to not be considered an edgeport. For example:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree edgeport disable
```

or

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#no spanning-tree edgeport
```

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

Use the **spanning-tree link-type** command to configure the spanning-tree protocol link type for an interface. To return to the default value, use the **no** form of this command.

Syntax Description

auto	Determines link type by the port's duplex settings.
point-to-point	Manually sets link type to point-to-point, regardless of duplex settings.
shared	Manually sets link type to shared, regardless of duplex settings.

Default Values

By default, a port is set to auto.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command overrides the default link-type setting determined by the duplex of the individual port. By default a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Using the **link-type auto** command, restores the convention of determining link-type based on duplex settings.

Usage Examples

The following example forces the link type to point-to-point, even if the port is configured to be half-duplex:

```
(config)#bridge 1 protocol ieee
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree link-type point-to-point
```

Technology Review

Rapid transitions are possible in rapid spanning-tree protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link type to **auto** allows the spanning tree to automatically configure the link type based on the duplex of the link. Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

spanning-tree path-cost *<value>*

Use the **spanning tree path-cost** command to assign a cost to a bridge group that is used when computing the spanning-tree root path. To return to the default path-cost value, use the **no** form of this command.

Syntax Description

<value>	Assigns a path cost value for spanning calculations to the bridge interface (valid range: 0 to 65,535).

Default Values

Be default, the path-cost value is set at 19.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The specified value is inversely proportional to the likelihood the bridge interface will be chosen as the root path. Set the path-cost value lower to increase the chance the interface will be the root. To obtain the most accurate spanning-tree calculations, develop a system for determining path costs for links and apply it to all bridged interfaces.

Usage Examples

The following example assigns a path cost of 100 for bridge group 17 on a Frame Relay sub-interface:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree path-cost 100
```

Technology Review

Spanning-tree protocol provides a way to prevent loopback or parallel paths in bridged networks. Using the priority values and path costs assigned to each bridging interface, the spanning-tree protocol determines the root path and identifies whether to block or allow other paths.

spanning-tree priority *<value>*

Use the **spanning-tree priority** command to select the priority level of a port associated with a bridge. To return to the default bridge-group priority value, use the **no** version of this command.

Syntax Description

<value>	Priority value for the bridge group; the lower the value, the higher the priority (valid range: 0 to 255).

Default Values

Be default, the bridge-group priority value is set at 28.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The only time that this priority level is used is when two interfaces with a path to the root have equal cost. At that point, the level set in this command will determine which port the bridge will use. Set the priority value lower to increase the chance the interface will be used.

Usage Examples

The following example sets the maximum priority on the Frame Relay sub-interface labeled 1.16 in bridge group 17:

```
(config)#interface frame-relay 1.16
(config-fr 1.16)#spanning-tree priority 0
```

HDLC COMMAND SET

To activate the HDLC mode, enter the **interface hdcl** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface hdlc 1
(config-hdlc 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 784

alias link<"text"> on page 787

bandwidth <value> on page 788

bridge-group <group#> on page 789

crypto map <mapname> on page 790

dial-backup commands on page 792

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 808

fair-queue <threshold> on page 810

hold-queue <queue size> out on page 811

ip commands begin on page 812

keepalive <seconds> on page 837

lldp receive on page 838

lldp send [management-address l port-description l system-capabilities l system-description l system-name l and-receive] on page 839 *max-reserved-bandwidth <percent>* on page 841

mtu <size> on page 842

qos-policy out <mapname> on page 843

snmp trap link-status on page 845

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic on an interface. Use the **no** form of this command to remove an access policy association.

> *Configured access policies will only be active if the* ***ip firewall*** *command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<policyname>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** *<policy name>*.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the HDLC interface labeled 1:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:
(config)#**ip policy-class UnTrusted**
(config-policy-class)#**allow list InWeb**

Associate the access list with the interface:
(config)#**interface hdlc 1**
(config-hdlc 1)#**access-policy UnTrusted**

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of the AOS using the **ip firewall** command.

Step 2:
Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a "range." Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a "don't care." For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:
Create an access policy that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>
All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>
All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>
All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#access-policy MatchAll
```

alias link *<"text">*

Each configured HDLC interface (when referenced using SNMP) contains a link (physical port) and a bundle (group of links). RFC1471 (for Link Connection Protocol) provides an interface table to manage lists of bundles and associated links. The **alias link** command provides the management station an identifying description for each link (HDLC physical).

Syntax Description

<*"text"*>	Describes the interface (for SNMP) by alphanumeric character string (must be encased in quotation marks).

Default Values

By default, the HDLC identification string appears as empty quotes. (" ")

Applicable Platforms

This command applies to the 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Functional Notes

The **alias link** string should be used to uniquely identify an HDLC link. Enter a string that clearly identifies the link.

Usage Examples

The following example defines a unique character string for the virtual HDLC interface (1):

```
(config)#interface hdlc 1
(config-ppp 1)#alias link "HDLC_link_1"
```

Technology Review

Please refer to RFC1990 for a more detailed discussion on HDLC links and bundles.

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Enter bandwidth in kbps.

Default Values

To view default values use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the HDLC interface to 10 Mbps:

```
(config)#interface hdlc 1
(config-hdlc 1)#bandwidth 10000
```

bridge-group *<group#>*

Use the **bridge-group** command to assign an interface to the specified bridge group. Use the **no** form of this command to remove the interface from the bridge group.

Syntax Description

<group#>	Specifies bridge group number (1 to 255) specified using the **bridge-group** command

Default Values

By default, there are no configured bridge groups.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1 bridge, Ethernet to Frame Relay sub-interface, etc.).

Usage Examples

The following example assigns the HDLC interface labeled 1 to bridge-group 1:

```
(config)#interface hdlc 1
(config-hdlc 1)#bridge-group 1
```

crypto map *<mapname>*

Use the **crypto map** command to associate crypto maps with the interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> NOTE *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

<mapname> Enter the crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

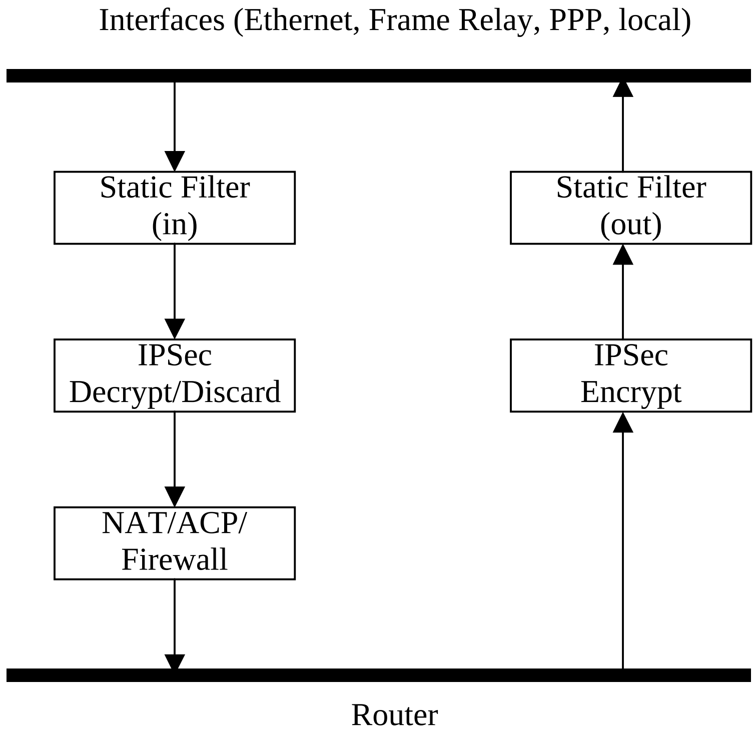
Command History

Release 9.1 Command was introduced.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following notes in mind.

When defining the policy-class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the un-encrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access-group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only un-encrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy-class on an interface. When specifying the ACLs for a crypto map, the source information is the private local-side, un-encrypted source of the data. The destination information will be the far-end, un-encrypted destination of the data. However, ACLs for a policy-class work in reverse. The source information for the ACL in a policy-class is the far-end. The destination information is the local-side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the HDLC 1 interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#crypto map MyMap
```

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the PPP interface to automatically attempt a dial-backup upon failure. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial-backup upon a failure.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example enables automatic dial-backup on the endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup auto-backup
```

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial-backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to automatically restore the primary connection when the failure condition clears:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup auto-restore
```

dial-backup backup-delay *<seconds>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

<seconds>	Specifies the delay period (in seconds) a failure must be active before the AOS will enter backup operation on the interface. Range: 10 to 86,400 seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 60 seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup backup-delay 60
```

dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]

Use the **dial-backup call-mode** command to combine user data with pattern data to ensure data does not mirror standard DDS loop codes (use only on 64 kbps circuits without Frame Relay signaling). Use the **no** form of this command to return to the default value.

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer.**

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Functional Notes

The majority of the configuration for PPP dial-backup is configured in the PPP interface's. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname "Remote3200"
enable password adtran
!
interface eth 0/1
  ip address  192.168.1.254  255.255.255.0
  no shutdown
!
interface modem 1/3
no shutdown
!
```

```
interface t1 1/1
coding b8zs
framing esf
clock source line
tdm-group 1 timeslots 1-24
no shutdown
!
interface ppp 1
ip address 10.1.1.2 255.255.255.252
dial-backup call-mode originate
dial-backup number 5551111 analog ppp 2
cross-connect 1 t1 1/1 1 ppp 1
!
interface ppp 2
description connected to corp for dial-backup
ip address 10.10.10.2 255.255.255.252
ppp authentication pap
ppp pap sent-username joe password pswrd
!
ip route 0.0.0.0  0.0.0.0  10.1.1.1
!
line telnet 0 4
password adtran
```

Sample configuration for central router (dialing in)

```
hostname "Central3200"
enable password adtran
!
interface eth 0/1
ip address  192.168.100.254  255.255.255.0
no shutdown
!
interface modem 1/3
no shutdown
!
interface t1 1/1
coding b8zs
framing esf
clock source line
tdm-group 1 timeslots 1-24
no shutdown
!
interface ppp 1
```

```
no shutdown
cross-connect 1 t1 1/1 1 ppp 1
ip address 10.1.1.1 255.255.255.252
dial-backup call-mode answer
dial-backup number 555-8888 analog ppp 2
!
interface ppp 2
description connection for remote 3200 dialin for backup
ip address 10.10.10.1 255.255.255.252
ppp authentication pap
username joe password pswrd
!
line telnet 0 4
password adtran
```

Usage Examples

The following example configures the AOS to answer dial-backup calls on this endpoint but never generate calls:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup call-mode answer-always
```

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial-backup, where in the configuration the AOS accesses specific routing information, etc.):

Dialing Out

1. The AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, the AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number <digits> [analog | digital-56k | digital 64k] <isdn min chan> <isdn max chan> <interface>* on page 801).
3. When placing the call, the AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, the AOS places a call to the second number if configured. The second number to be dialed references a separate PPP interface.

Dialing In

1. The AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and the AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from Caller ID, the call is terminated.

dial-backup connect-timeout *<seconds>*

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

<seconds>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call (valid range: 10 to 300).

Default Values

By default, the **dial-backup connect-timeout** period is set to 60 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 120 seconds before retrying a failed dial-backup call:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup connect-timeout 120
```

dial-backup force [backup | primary]

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer* | *answer-always* | *originate* | *originate-answer* | *originate-answer-always]* on page 795.

Syntax Description

backup	Force backup regardless of primary link state.
primary	Force primary link regardless of its state.

Default Values

By default, this feature is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to force this interface into dial-backup:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup force backup
```

dial-backup maximum-retry *<attempts>*

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

<attempts>	Selects the number of call retries that will be made after a link failure (valid range: 0 to 15). Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to 0 attempts.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to retry a dial-backup call four times before considering backup operation not available:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup maximum-retry 4
```

dial-backup number *<digits>* [analog | digital-56k | digital 64k] *<isdn min chan> <isdn max chan> <interface>*

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

<digits>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates number connects to an analog modem.
digital-56k	Indicates number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates number belongs to a digital 64 kbps per DS0 connection.
<isdn min chan>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection (Range: 1 to 24).
<isdn mas chan>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection (Range: 1 to 24).
<interface>	Specifies the PPP interface (e.g., PPP 3) to use when originating or answering using this number.

Default Values

By default, there are no configured dial-backup numbers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to dial 704-555-1212 (digital 64 kbps connection) to initiate dial-backup operation on this endpoint using interface PPP 3:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup number 7045551212 digital-64k 1 1 ppp 3
```

dial-backup priority *<value>*

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

<value>	Sets the relative priority of this link (valid range: 0 to 100). A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to 50.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example assigns the highest priority to this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup priority 100
```

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

No subcommands.

Default Values

By default, the AOS does not randomize the dial-backup call timers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to randomize the dial-backup timers associated with this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup randomize-timers
```

dial-backup redial-delay *<seconds>*

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

<seconds>	Specifies the delay in seconds between attempting to re-dial a failed backup attempt. Range: 10 to 3600.

Default Values

By default, **dial-backup redial-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures a redial delay of 25 seconds on this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup redial-delay 25
```

dial-backup restore-delay *<seconds>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is “bouncing” in and out of alarm. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

<seconds>	Specifies the number of seconds the AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range: 10 to 86,400.

Default Values

By default, **dial-backup restore-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 30 seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup restore-delay 30
```

dial-backup schedule [day | enable-time | disable-time]

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial-backup (as specified). For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 795.

Syntax Description

day	Sets the days to allow backup (valid range: Monday through Sunday).
enable-time	Sets the time of day to enable backup. Time is entered in 24-hour format (00:00).
disable-time	Sets the time of day to disable backup.

Default Values

By default, dial-backup is enabled for all days and times if the dial-backup auto-backup command has been issued and the dial-backup schedule has not been entered.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example enables dial-backup Monday through Friday 8:00 am to 7:00 pm:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup schedule enable-time 08:00
(config-ppp 1)#dial-backup schedule disable-time 19:00
(config-ppp 1)#no dial-backup schedule day Saturday
(config-ppp 1)#no dial-backup schedule day Sunday
```

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example deactivates the configured dial-backup interface:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup shutdown
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

See **Functional Notes** below for syntax descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A web-based interface provides two levels of control over your domain, catering to average or power users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service, in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address doesn't change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name) Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com) you need Custom DNS service which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the dynamic-dns to **dyndns-custom** with hostname **host**, username **user**, and password **pass**:

```
(config)#interface hdlc 1
(config-hdlc 1)#dynamic-dns dyndns-custom host user pass
```

fair-queue *<threshold>*

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable FIFO (first-in-first-out) queueing for an interface. WFQ is enabled by default for WAN interfaces.

Syntax Description

<threshold>	Optional. Value that specifies the maximum number of packets that can be present in each conversation sub-queue. Packets received for a conversation after this limit is reached are discarded. Range: 16 to 512.

Default Values

By default, fair-queue is enabled with a threshold of 64 packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

```
(config)#interface hdlc 1
(config-hdlc 1)#fair-queue 100
```

hold-queue *<queue size>* out

Use the **hold-queue** command to change the overall size of an interface's WAN output queue.

Syntax Description

<queue size>	The total number of packets the output queue can contain before packets are dropped. Range: 16 to 1000.

Default Values

The default queue size for WFQ is 400. The default queue size for PPP FIFO and Frame Relay round-robin is 200.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example sets the overall output queue size to 700:

```
(config)#interface hdlc 1
(config-hdlc 1)#hold-queue 700
```

ip access-group *<listname>* [**in | out**]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Assigned IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the unit to only allow Telnet traffic (as defined in the user-configured **TelnetOnly** IP access list) into the HDLC interface:

```
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#int hdlc 1
(config-hdlc 1)#ip access-group TelnetOnly in
```

ip address *<address> <mask>* secondary

Use the **ip address** command to define an IP address on the specified interface. Use the optional **secondary** keyword to define a secondary IP address. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<mask>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Keyword used to configure a secondary IP address for the specified interface.

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced

Functional Notes

Use secondary IP addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IP addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IP addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IP address of **192.22.72.101/30**:

```
(config)#hdlc 1
(config-hdlc 1)#ip address 192.22.72.101 255.255.255.252 secondary
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure the AOS to forward UDP broadcast packets. See ip forward-protocol udp <port number>* on page 378 *for more information.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets.

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper-address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address 192.33.5.99:

```
(config)#ip forward-protocol udp domain
(config)#interface hdlc 1
(config-hdlc 1)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description

immediate-leave	If only one host (or IGMP snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval <*milliseconds*>	This command controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65535 ms. Default: 1000 ms.
querier-timeout <*seconds*>	Number of seconds that the router waits after the current querier’s last query before it takes over as querier (IGMP V2). Range: 60-300 seconds. Default: 2x the **query-interval** value.
query-interval <*seconds* >	Interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65535 seconds. Default: 60 seconds.
query-max-response-time <*seconds*>	Maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group <*group-address*>	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface’s IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding. See *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub upstream* on page 820 for more information.

Usage Examples

The following example enables multicast forwarding and IGMP on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip mcast-stub downstream
```

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the IGMP proxy. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 10.1	Command was expanded to include HDLC interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy. Refer to *ip mcast-stub helper-address <ip address>* on page 387, *ip mcast-stub downstream* on page 818, and *ip mcast-stub upstream* on page 820 for more information.

Usage Examples

The following example sets the helper address as the IGMP proxy:

```
config)#interface hdlc 1
(config-hdlc 1)#ip mcast-stub helper-enable
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface. See *ip mcast-stub helper-address <ip address>* on page 387 and *ip mcast-stub downstream* on page 818 for more information.

Usage Examples

The following example enables multicast forwarding on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key	Specifies a simple-text authentication password to be used by other routers using <*password*> the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 1 to 65535.
dead-interval <*seconds*>	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range: 0 to 32767.
hello-interval <*seconds*>	Specifies the interval between hello packets sent on the interface. Range: 0 to 32767.
message-digest-key <*keyid*> **md5** <*key*>	Configures OSPF Message Digest 5 (MD5) authentication (16-byte max) keys.
priority <*value*>	Set the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0 to 255.
retransmit-interval <*seconds*>	Specifies the time between link-state advertisements (LSAs). Range: 0 to 32767.
transmit-delay <*seconds*>	Sets the estimated time required to send an LSA on the interface. Range: 0 to 32767.

Default Values

retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second
hello-interval <*seconds*>	10 seconds: Ethernet, point-to-point, Frame Relay, and PPP
dead-interval <*seconds*>	40 seconds

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Example

The following example sets the maximum number of seconds allowed between hello packets to 25,000:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip ospf dead-interval 25000
```

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Select message-digest authentication type.
null	Optional. Select for no authentication to be used.

Default Values

By default, this is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example specifies that no authentication will be used on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Set the network type for broadcast.
point-to-point	Set the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP and Frame Relay default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip ospf network broadcast
```

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM Sparse Mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the HDLC 1 interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip pim sparse-mode
```

ip pim-sparse dr-priority *<priority number>*

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the routers priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<priority number>	Specifies the priority number for the DR router. Valid range is 1 to 4,294,967,295.

Default Values

By default, the DR priority is set to 1.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the DR priority to 5:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip pim-sparse dr-priority 5
```

ip pim-sparse hello-timer *<time>*

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time in seconds between hello transmissions. Valid range is 10 to 12,600 seconds.

Default Values

By default, the hello timer is set to 30 seconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the hello timer to 60 seconds:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip pim-sparse hello-timer 60
```

ip pim-sparse nbr-timeout *<time>*

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is 30 to 10,800 seconds.

Default Values

By default, the nbr-timeout is set to 105 seconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip pim-sparse nbr-timeout 300
```

ip pim-sparse override-interval *<time>*

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the LAN may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the delay time in milliseconds. Valid range is 0 to 65,535 milliseconds.

Default Values

By default, the override-interval is set to 2500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override-interval to 3000 milliseconds:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip pim-sparse override-interval 3000
```

ip pim-sparse propagation-delay *<time>*

Use the **ip pim-sparse propagation-delay** command to specify protocol-independent multicast (PIM) sparse join/prune propagation delay. This is the expected propagation delay in milliseconds over the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the expected propagation delay in milliseconds. Valid range is 0 to 32,767 milliseconds.

Default Values

By default, the propagation-delay is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation-delay to 1000 milliseconds:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip pim-sparse propagation-delay 1000
```

ip policy route-map *<policy name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<policy name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Applicable Platforms

This command applies to the NetVanta 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the HDLC 1 interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip policy route-map policy1
```

ip proxy-arp *<ip address> <subnet mask>*

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<ip address>	Defines the proxy ARP IP address in dotted decimal notation (for example: 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy-arp is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, the AOS will respond to all proxy ARP requests with its specified MAC address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following enables proxy ARP on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Only accept received RIP version 1 packets on the interface.
2	Only accept received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the version command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. See *version [1 | 2]* on page 1144 for more information.

The AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the HDLC interface to accept only RIP version 2 packets:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Only transmits RIP version 1 packets on the interface.
2	Only transmits RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. See *version [1 | 2]* on page 1144 for more information.

The AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the HDLC interface to transmit only RIP version 2 packets:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip rip send version 2
```

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route-cache is enabled for all virtual PPP interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#ip route-cache
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface (in the format **type slot/port**) that contains the IP address to use as the source address for all packets transmitted on this interface.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command was expanded to include demand interface.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the Frame Relay Sub-Interface Configuration mode configures the Frame Relay sub-interface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, the AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the HDLC interface to use the IP address assigned to the Ethernet interface (**eth 0/1**):

```
(config)#interface hdlc 1
(config-hdlc 1)#ip unnumbered eth 0/1
```

keepalive *<seconds>*

Use the **keepalive** command to enable the transmission of keepalive packets on the interface and specify the time interval in seconds between transmitted packets.

Syntax Description

<seconds>	Defines the time interval (in seconds) between transmitted keepalive packets (valid range: 0 to 32,767 seconds).

Default Values

By default, the time interval between transmitted keepalive packets is 10 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

If three keepalive packets are sent to an interface with no response, the interface is considered down. To detect interface failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of 5 seconds on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#keepalive 5
```

lldp receive

Use the **lldp receive** command to allow LLDP packets to be received on this interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the HDLC interface to receive LLDP packets:

```
(config)#interface hdlc 1
(config-hdlc 1)#lldp receive
```

lldp send [management-address | port-description | system-capabilities | system-description | system-name | and-receive]

Use the **lldp send** command to configure this interface to transmit LLDP packets or to control the types of information contained in the LLDP packets transmitted by this interface.

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

Be default, all interfaces are configured to transmit and receive LLDP packets of all types.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the HDLC interface to transmit LLDP packets containing all enabled information types:

```
(config)#interface hdlc 1
(config-hdlc 1)#lldp send
```

The following example configures the HDLC to transmit and receive LLDP packets containing all information types:

```
(config)#interface hdlc 1
(config-hdlc 1)#lldp send and-receive
```

max-reserved-bandwidth *<percent>*

Use the **max-reserved-bandwidth** command to define the maximum amount of interface bandwidth reserved for Quality of Service (QoS). Use the **no** form of this command to return to the default value.

Syntax Description

<percent>	Specifies the maximum amount of bandwidth to reserve for QoS. This setting is configured as a percentage of the total interface speed. Range: 1 to 100 percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the **reserved-bandwidth** maximum at 80 percent:

```
(config)#interface hdlc 1
(config-hdlc 1)#max-reserved-bandwidth 80
```

mtu <*size*>

Use the **mtu** command to configure the maximum transmit unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<*size*> Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:

ATM interfaces	64 to 1520
Demand interfaces	64 to 1520
Ethernet interfaces	64 to 1500
FDL interfaces	64 to 256
HDLC interfaces	64 to 1520
Loopback interfaces	64 to 1500
Tunnel interfaces	64 to 18,190
Virtual Frame Relay sub-interfaces	64 to 1520
Virtual PPP interfaces	64 to 1500

Default Values

<*size*> The default values for the various interfaces are listed below:

ATM interfaces	1500
Demand interfaces	1500
Ethernet interfaces	1500
FDL interfaces	256
HDLC interfaces	1500
Loopback interfaces	1500
Tunnel interfaces	1500
Virtual Frame Relay sub-interfaces	1500
Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#mtu 1200
```

qos-policy out *<mapname>*

Use the **qos-policy out** command to apply a previously-configured QoS map to an interface. Use the **no** form of this command to remove the map from the interface. The **out** keyword specifies that this policy will be applied to outgoing packets.

Syntax Description

<mapname>	Specifies the name of a previously-created QoS map (see *qos map <mapname> <sequence number>* on page 434 for more information).

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross-connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when ADSL finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#qos-policy out VOICEMAP
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the HDLC interface:

```
(config)#interface hdlc 1
(config-hdlc 1)#no snmp trap link-status
```

LOOPBACK INTERFACE CONFIGURATION COMMAND SET

To activate the Loopback Interface Configuration mode, enter the **interface loopback** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface loopback 1
(config-loop 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 847

bandwidth <value> on page 850

crypto map <mapname> on page 851

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 853

ip commands begin on page 855

ip commands begin on page 856

mtu <size> on page 880

snmp trap on page 881

snmp trap link-status on page 882

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic to an interface. Use the **no** form of this command to remove an access policy association.

> NOTE *Configured access policies will only be active if the **ip firewall** command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<policyname>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 6.1	Command was expanded to include NetVanta 1000 and 2000 units.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** *<policy name>*.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the loopback interface:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:
(config)#**ip policy-class UnTrusted**
(config-policy-class)#**allow list InWeb**

Associate the access policy with the loopback interface:
(config)#**interface loopback 1**
(config-loop 1)#**access-policy UnTrusted**

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:
Enable the security features of the AOS using the **ip firewall** command.

Step 2:
Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:
Create an IP policy class that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (access list) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>
All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>
All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>
All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> interface <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the loopback interface labeled 1:

```
(config)#interface loopback 1
(config-loop 1)#access-policy MatchAll
```

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies bandwidth in kbps.

Default Values

To view default values, use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the loopback interface to 10 Mbps:

```
(config)#interface loopback 1
(config-loop 1)#bandwidth 10000
```

crypto map *<mapname>*

Use the **crypto map** command to associate crypto maps with the interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> NOTE *For VPN configuration example scripts, refer to the technical support note **Configuring VPN** located on the **ADTRAN OS Documentation** CD provided with your unit.*

Syntax Description

<mapname>	Specifies the crypto map name that you wish to assign to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

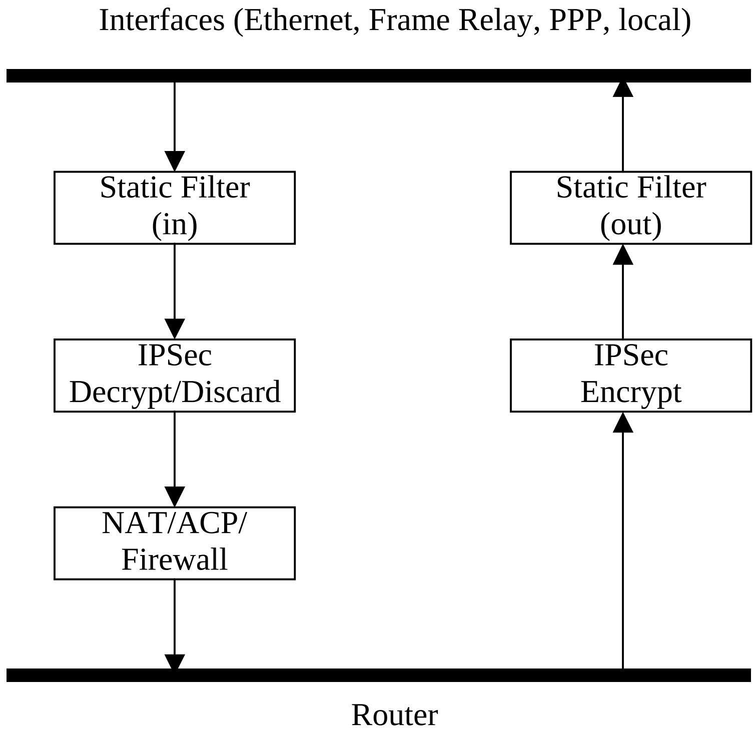
Command History

Release 4.1	Command was introduced.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following information in mind:

When defining the policy class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local side, unencrypted source of the data. The destination information will be the far end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local-side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the loopback interface:

```
(config)#interface loopback 1
(config-loop 1)#crypto map MyMap
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

See *Functional Notes*, below, for argument descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A web-based interface provides two levels of control over your domain, catering to average or power users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file, allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address doesn't change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name), Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the dynamic-dns to dyndns-custom with hostname **host**, username **user**, and password **pass**:

```
(config)#interface loopback 1
(config-loop 1)#dynamic-dns dyndns-custom host user pass
```

ip access-group *<listname>* [**in | out**]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Specifies IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to allow only Telnet traffic into the loopback interface:

```
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#interface loopback 1
(config-loop 1)#ip access-group TelnetOnly in
```

ip address *<address> <mask>* secondary

Use the **ip address** command to define an IP address on the specified interface. Use the optional **secondary** keyword to define a secondary IP address. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<mask>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Configures a secondary IP address for the specified interface.

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 2.1	Added **ip address dhcp** for DHCP client support.

Functional Notes

Use secondary IP addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IP addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IP addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IP address of **192.22.72.101/30**:

```
(config)#interface loopback 1
(config-loop 1)#ip address 192.22.72.101 255.255.255.252 secondary
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper** command must be used in conjunction with the **ip forward-protocol** command to configure the AOS to forward UDP broadcast packets. See ip forward-protocol udp <port number>* on page 378 *for more information.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets.

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper-address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address 192.33.5.99:

```
(config)#ip forward-protocol udp domain
(config)#interface loopback 1
(config-loop 1)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description

immediate-leave	If only one host (or IGMP snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval *<milliseconds>*	This command controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65535 ms. Default: 1000 ms.
querier-timeout *<seconds>*	Number of seconds that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range: 60 to 300 seconds. Default: 2x the **query-interval** value.
query-interval *<seconds >*	Interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65535 seconds. Default: 60 seconds.
query-max-response-time *<seconds>*	Maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group *<group-address>*	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface's IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
(config)#interface loopback 1
(config-loop 1)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface loopback 1
(config-loop 1)#ip mcast-stub downstream
```

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the IGMP proxy. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include loopback interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy.

Usage Examples

The following example sets the helper address as the IGMP proxy:

```
(config)#interface loopback 1
(config-loop 1)#ip mcast-stub helper-enable
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface loopback 1
(config-loop 1)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key	Specifies a simple-text authentication password to be used by other routers using *<password>* the OSPF simple password authentication.
cost *<value>*	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 1 to 65,535.
dead-interval *<seconds>*	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range: 0 to 32,767.
hello-interval *<seconds>*	Specifies the interval between hello packets sent on the interface. Range: 0 to 32767.
message-digest-key *<keyid>* **md5** *<key>*	Configures OSPF Message Digest 5 (MD5) authentication (16-byte max) keys.
priority *<value>*	Set the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0 to 255.
retransmit-interval *<seconds>*	Specifies the time between link-state advertisements (LSAs). Range: 0 to 32,767.
transmit-delay *<seconds>*	Sets the estimated time required to send an LSA on the interface. Range: 0 to 32,767.

Default Values

retransmit-interval *<seconds>*	5 seconds
transmit-delay *<seconds>*	1 second
hello-interval *<seconds>*	10 seconds: Ethernet, point-to-point, Frame Relay, and PPP
dead-interval *<seconds>*	40 seconds

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Example

The following example sets the maximum number of seconds allowed between hello packets to 25,000:

```
(config)#interface loopback 1
(config-loop 1)#ip ospf dead-interval 25000
```

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Specifies the message-digest authentication type.
null	Optional. Specifies for no authentication to be used.

Default Values

By default, this is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example specifies that no authentication will be used on the loopback interface:

```
(config)#interface loopback 1
(config-loop 1)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP and Frame Relay default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface loopback 1
(config-loop 1)#ip ospf network broadcast
```

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM Sparse Mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

```
(config)#interface loopback 1
(config-loop 1)#ip pim sparse-mode
```

ip pim-sparse dr-priority *<priority number>*

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the routers priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<priority number>	Specifies the priority number for the DR router. Valid range is 1 to 4,294,967,295.

Default Values

By default, the DR priority is set to 1.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the DR priority to 5:

```
((config)#interface loopback 1
(config-loop 1)#ip pim-sparse dr-priority 5
```

ip pim-sparse hello-timer *<time>*

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the time in seconds between hello transmissions. Valid range is 10 to 12,600 seconds.

Default Values

By default, the hello timer is set to 30 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the hello timer to 60 seconds:

```
(config)#interface loopback 1
(config-loop 1)#ip pim-sparse hello-timer 60
```

ip pim-sparse nbr-timeout *<time>*

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is 30 to 10,800 seconds.

Default Values

By default, the nbr-timeout is set to 105 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

```
(config)#interface loopback 1
(config-loop 1)#ip pim-sparse nbr-timeout 300
```

ip pim-sparse override-interval *<time>*

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the LAN may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the delay time in milliseconds. Valid range is 0 to 65,535 milliseconds.

Default Values

By default, the override-interval is set to 2500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override-interval to 3000 milliseconds:

```
(config)#interface loopback 1
(config-loop 1)#ip pim-sparse override-interval 3000
```

ip pim-sparse propagation-delay *<time>*

Use the **ip pim-sparse propagation-delay** command to specify protocol-independent multicast (PIM) sparse join/prune propagation delay. This is the expected propagation delay in milliseconds over the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<time> Specifies the expected propagation delay in milliseconds. Valid range is 0 to 32,767 milliseconds.

Default Values

By default, the propagation-delay is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1 Command was introduced.

Usage Examples

The following example sets the propagation-delay to 1000 milliseconds:

```
(config)#interface loopback 1
(config-loop 1)#ip pim-sparse propagation-delay 1000
```

ip policy route-map *<policy name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<policy name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

```
(config)#interface loopback 1
(config-loop 1)#ip policy route-map policy1
```

ip proxy-arp *<address> <subnet mask>*

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy arp is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy-arp allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy-arp is enabled, the AOS will respond to all proxy-arp requests with its specified MAC address and forward packets accordingly.

Enabling proxy-arp on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following enables proxy-arp on the loopback interface:

```
(config)#interface loopback 1
(config-loop 1)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface.

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

The AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the loopback interface to accept only RIP version 2 packets:

```
(config)#interface loopback 1
(config-loop 1)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface.

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

The AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the loopback interface to transmit only RIP version 2 packets:

```
(config)#interface loopback 1
(config-loop 1)#ip rip send version 2
```

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> NOTE *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route-cache is enabled for all virtual PPP interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the loopback interface:

```
(config)#interface loopback 1
(config-loop 1)#ip route-cache
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface in the format **type slot/port** (e.g., **ppp 1**) that contains the IP address to be used as the source address for all packets transmitted on this interface. Enter **ip unnumbered ?** for a complete list of valid interfaces.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include demand interfaces.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered ppp 1** while in the Ethernet Interface Configuration mode configures the Ethernet interface to use the IP address assigned to the PPP interface for all IP processing. In addition, the AOS uses the specified interface information when sending route updates over the unnumbered interface.

Usage Examples

The following example configures the loopback interface (labeled **loop 1**) to use the IP address assigned to the PPP interface (**ppp 1**):

```
(config)#interface loopback 1
(config-loop 1)#ip unnumbered ppp 1
```

mtu *<size>*

Use the **mtu** command to configure the maximum transmit unit size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size> Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:

ATM interfaces	64 to 1520
Demand interfaces	64 to 1520
Ethernet interfaces	64 to 1500
FDL interfaces	64 to 256
HDLC interfaces	64 to 1520
Loopback interfaces	64 to 1500
Tunnel interfaces	64 to 18,190
Virtual Frame Relay sub-interfaces	64 to 1520
Virtual PPP interfaces	64 to 1500

Default Values

<size> The default values for the various interfaces are listed below:

ATM interfaces	1500
Demand interfaces	1500
Ethernet interfaces	1500
FDL interfaces	256
HDLC interfaces	1500
Loopback interfaces	1500
Tunnel interfaces	1500
Virtual Frame Relay sub-interfaces	1500
Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1 Command was introduced.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the loopback interface:

```
(config)#interface loopback 1
(config-loop 1)#mtu 1200
```

snmp trap

Use the **snmp trap** command to enable all supported Simple Network Management Protocol (SNMP) traps on the interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces (except virtual Frame Relay interfaces and sub-interfaces) have SNMP traps enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Ethernet sub-interfaces and Gigabit Ethernet interfaces.

Usage Examples

The following example enables SNMP capability on the Ethernet interface:

```
(config)#interface eth 0/1
(config-eth 0/1)#snmp trap
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the loopback interface:

```
(config)#interface loopback 1
(config-loop 1)#no snmp trap link-status
```

PPP INTERFACE CONFIGURATION COMMAND SET

To activate the PPP Interface Configuration mode, enter the **interface ppp** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface ppp 1
(config-ppp 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 885

alias link<"text"> on page 888

bandwidth <value> on page 889

bridge-group commands begin on page 890

crypto map <mapname> on page 896

dial-backup commands begin on page 898

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 915

fair-queue <threshold> on page 917

hold-queue <queue size> out on page 918

ip commands begin on page 919

keepalive <seconds> on page 945

lldp receive on page 946

lldp send [management-address l port-description l system-capabilities l system-description l system-name l and-receive] on page 947 *max-reserved-bandwidth <percent>* on page 949

mtu <size> on page 950

peer default ip address <address> on page 951

ppp commands begin on page 952

pppoe ac-name <name> on page 961

pppoe service-name <name> on page 962

qos-policy out <mapname> on page 963

snmp trap link-status on page 965

username <username> password <password> on page 966

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic to an interface. Use the **no** form of this command to remove an access policy association.

> NOTE *Configured access policies will only be active if the* ***ip firewall*** *command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<policyname>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 6.1	Command was expanded to include NetVanta 1000 and 2000 units.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** *<policy name>*.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the virtual PPP interface:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:

```
(config)#ip policy-class UnTrusted
(config-policy-class)#allow list InWeb
```

Associate the access list with the PPP virtual interface (labeled 1):

```
(config)#interface ppp 1
(config-ppp 1)#access-policy UnTrusted
```

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:

Enable the security features of the AOS using the **ip firewall** command.

Step 2:

Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a “range.” Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a “don’t care.” For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:

Create an access policy that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>

All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>

All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the virtual PPP interface labeled 1:

```
(config)#interface ppp 1
(config-ppp 1)#access-policy MatchAll
```

alias link<*"text"*>

Each configured PPP interface (when referenced using SNMP) contains a link (physical port) and a bundle (group of links). RFC1471 (for Link Connection Protocol) provides an interface table to manage lists of bundles and associated links. The **alias link** command provides the management station an identifying description for each link (PPP physical).

Syntax Description

<*"text"*>	Describes the interface (for SNMP) by alphanumeric character string (must be encased in quotation marks).

Default Values

By default, the PPP identification string appears as empty quotes. (" ")

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

The **alias link** string should be used to uniquely identify a PPP link. Enter a string that clearly identifies the link.

Usage Examples

The following example defines a unique character string for the virtual PPP interface (1):

```
(config)#interface ppp 1
(config-ppp 1)#alias link "PPP_link_1"
```

Technology Review

Please refer to RFC1990 for a more detailed discussion on PPP links and bundles.

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies the bandwidth value in kbps.

Default Values

To view default values, use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the PPP interface to 10 Mbps:

```
(config)#interface ppp 1
(config-ppp 1)#bandwidth 10000
```

bridge-group *<group#>*

Use the **bridge-group** command to assign an interface to the specified bridge group. This command is supported on all Ethernet interfaces, PPP virtual interfaces, and Frame Relay virtual sub-interfaces.

Syntax Description

<group#>	Assigns a bridge group number (range: 1 to 255).

Default Values

By default, there are no configured bridge groups.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

A bridged network can provide excellent traffic management to reduce collisions and limit the amount of bandwidth wasted with unnecessary transmissions when routing is not necessary. Any two interfaces can be bridged (Ethernet to T1 bridge, Ethernet to Frame Relay sub-interface, etc.).

Usage Examples

The following example assigns the PPP interface to bridge-group 1:

```
(config)#interface ppp 1
(config-ppp 1)#bridge-group 1
```

bridge-group *<group#>* bpdufilter [enable | disable]

Use the **bridge-group bpdufilter** command to block BPDUs from being transmitted and received on this interface. To return to the default value, use the **no** form of this command.

Syntax Description

<group#>	Assigns a bridge group number (range: 1 to 255).
enable	Enables the BPDU filter.
disable	Disables the BPDU filter.

Default Values

By default, this command is set to disable.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The purpose of this command is to remove a port from participation in the spanning tree. This might be beneficial while debugging a network setup. It normally should not be used in a live network.

Usage Examples

The following example enables the BPDU filter on the interface:

```
(config)#interface ppp 1
(config-ppp 1)#bridge-group 1 bpdufilter enable
```

bridge-group *<group#>* bpduguard [enable | disable]

Use the **bridge-group bpduguard** command to block BPDUs from being received on this interface. To return to the default value, use the **no** form of this command.

Syntax Description

<group#>	Assigns a bridge group number (range: 1 to 255).
enable	Enables the BPDU block.
disable	Disables the BPDU block.

Default Values

By default, this command is set to disable.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables the BPDU guard on the interface:

```
(config)#interface ppp 1
(config-ppp 1)#bridge-group 1 bpduguard enable
```

bridge-group *<group#>* edgeport [disable]

Use the **bridge-group edgeport** command to set this interface to be an edgeport. This configures the interface to go to a forwarding state when the link goes up. To return to the default value, use the **no** form of this command.

Syntax Description

<group#>	Assigns a bridge group number (range: 1 to 255).
disable	Optional. Configures the interface to not be the edgeport by default. This command is designed to override the global setting of the *bridge <group#> protocol ieee* on page 304.

Default Values

By default, this command is set to disable.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures the interface to be an edgeport:

```
(config)#interface ppp 1
(config-ppp 1)#bridge-group 1 edgeport
```

An individual interface can be configured to not be considered an edgeport. For example:

```
(config)#interface ppp 1
(config-ppp 1)#bridge-group 1 edgeport disable
or
(config)#interface ppp 1
(config-ppp 1)#no bridge-group 1 edgeport
```

bridge-group *<group#>* link-type [auto | point-to-point | shared]

Use the **bridge-group link-type** command to configure the spanning-tree protocol link type for an interface. To return to the default value, use the **no** form of this command.

Syntax Description

<group#>	Assigns a bridge group number (range: 1 to 255).
auto	Determines link type by the port's duplex settings.
point-to-point	Manually sets link type to point-to-point, regardless of duplex settings.
shared	Manually sets link type to shared, regardless of duplex settings.

Default Values

By default, a port is set to auto.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command overrides the default link-type setting determined by the duplex of the individual port. By default a port configured for half-duplex is set to **shared** link type, and a port configured for full-duplex is set to **point-to-point** link type. Setting the link type manually overrides the default and forces the port to use the specified link type. Using the **link-type auto** command restores the convention of determining link type based on duplex settings.

Usage Examples

The following example forces the link type to point-to-point, even if the port is configured to be half-duplex:

```
(config)#bridge 1 protocol ieee
(config)#interface ppp 1
(config-ppp 1)#bridge-group 1 link-type point-to-point
```

Technology Review

Rapid transitions are possible in rapid spanning-tree protocol (RSTP) by taking advantage of point-to-point links (a port is connected to exactly one other bridge) and edge-port connections (a port is not connected to any additional bridges). Setting the link type to **auto** allows the spanning tree to automatically configure the link type based on the duplex of the link. Setting the link type to **point-to-point** allows a half-duplex link to act as if it were a point-to-point link.

bridge-group *<group#>* spanning-disabled

Use the **bridge-group spanning-disabled** command to transparently bridge two interfaces on a network (that have no parallel or redundant paths) without the overhead of spanning-tree protocol calculations. To enable the spanning-tree protocol on an interface, use the **no** form of this command.

Syntax Description

<group#>	Assigns a bridge group number (range: 1 to 255).

Default Values

By default, spanning-tree protocol is enabled on all created bridge groups.

Applicable Platforms

This command applies to the NetVanta 5000 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

When no parallel (redundant) paths exist within a bridged network, disabling the spanning tree protocol reduces traffic on the bridged interface. This traffic reduction can be helpful when bridging over a WAN link.

> *Before disabling the spanning-tree protocol on a bridged interface, verify that no redundant loops exist.*

Usage Examples

The following example disables the spanning-tree protocol for bridge group 17 on the PPP interface labeled 1:

```
(config)#interface ppp 1
(config-ppp 1)#bridge-group 17 spanning-disabled
```

Technology Review

Spanning-tree protocol provides a way to prevent loopback or parallel paths in bridged networks. Using the priority values and path costs assigned to each bridging interface, the spanning-tree protocol determines the root path and identifies whether to block or allow other paths.

crypto map *<mapname>*

Use the **crypto map** command to associate crypto maps with the interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> NOTE *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

<mapname>	Assigns a crypto map name to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

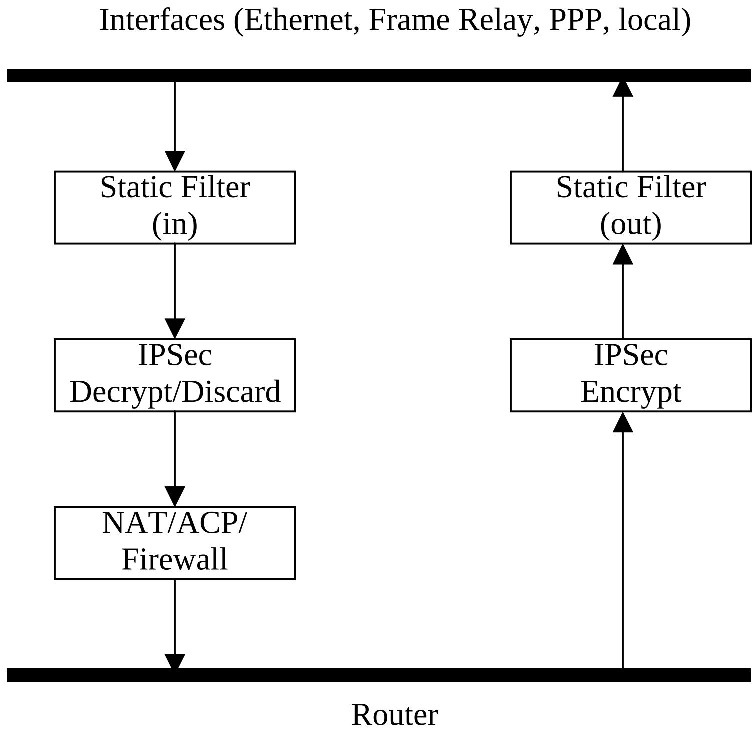
Command History

Release 4.1	Command was introduced.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following notes in mind.

When defining the policy class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local-side, unencrypted source of the data. The destination information will be the far end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#crypto map MyMap
```

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the PPP interface to automatically attempt a dial-backup upon failure. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial-backup upon a failure.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example enables automatic dial-backup on the endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup auto-backup
```

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial-backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to automatically restore the primary connection when the failure condition clears:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup auto-restore
```

dial-backup backup-delay *<seconds>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

<seconds>	Specifies the delay period (in seconds) a failure must be active before the AOS will enter backup operation on the interface. Range: 10 to 86,400 seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 60 seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup backup-delay 60
```

dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]

Use the **dial-backup call-mode** command to combine user data with pattern data to ensure data does not mirror standard DDS loop codes (use only on 64 kbps circuits without Frame Relay signaling). Use the **no** form of this command to return to the default value.

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer.**

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Functional Notes

The majority of the configuration for PPP dial-backup is configured in the PPP interfaces. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname "Remote3200"
enable password adtran
!
interface eth 0/1
  ip address  192.168.1.254  255.255.255.0
  no shutdown
!
interface modem 1/2
no shutdown
!
```

```
interface t1 1/1
coding b8zs
framing esf
clock source line
tdm-group 1 timeslots 1-24 speed 64
no shutdown
!
interface ppp 1
description Primary Interface for Connection to Central 3200
ip address 10.1.1.2 255.255.255.252
dial-backup call-mode originate
dial-backup number 5551111 analog ppp 2
cross-connect 1 t1 1/1 1 ppp 1
no shutdown
!
interface ppp 2
description Dial-Backup Interface for Connection to Central 3200
ip address 10.10.10.2 255.255.255.252
ppp pap sent-username joe password pswrd
no shutdown
!
ip route 0.0.0.0 0.0.0.0 ppp 1
ip route 0.0.0.0 0.0.0.0 ppp 2 100
!
!
line con 0
  no login
!
line telnet 0 4
  login
  password adtran
!
end
```

Sample configuration for central router (dialing in)

```
hostname "Central3200"
enable password adtran
!
interface eth 0/1
ip address 192.168.100.254 255.255.255.0
no shutdown
!
interface modem 1/2
```

```
no shutdown
!
interface t1 1/1
coding b8zs
framing esf
clock source internal
tdm-group 1 timeslots 1-24 speed 64
no shutdown
!
interface ppp 1
description Primary Interface for Connection to Remote 3200
cross-connect 1 t1 1/1 1 ppp 1
ip address 10.1.1.1 255.255.255.252
dial-backup call-mode answer
dial-backup number 5558888 analog ppp 2
no shutdown
!
interface ppp 2
description Dial-Backup Interface for Connection to Remote 3200
ip address 10.10.10.1 255.255.255.252
ppp authentication pap
username joe password pswrd
no shutdown
!
ip route 0.0.0.0 0.0.0.0 ppp 1
ip route 0.0.0.0 0.0.0.0 ppp 2 100
!
!
line con 0
 no login
!
line telnet 0 4
 login
 password adtran
!
end
```

Usage Examples

The following example configures the AOS to answer dial-backup calls on this endpoint but never generate calls:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup call-mode answer-always
```

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial-backup, where in the configuration the AOS accesses specific routing information, etc.):

Dialing Out

1. The AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, the AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number <digits> [analog | digital-56k | digital 64k] <isdn min chan> <isdn max chan> <interface>* on page 908).
3. When placing the call, the AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, the AOS places a call to the second number if configured. The second number to be dialed references a separate PPP interface.

Dialing In

1. The AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and the AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from Caller ID, the call is terminated.

dial-backup connect-timeout *<seconds>*

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

<seconds>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call (valid range: 10 to 300).

Default Values

By default, the **dial-backup connect-timeout** period is set to 60 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 120 seconds before retrying a failed dial-backup call:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup connect-timeout 120
```

dial-backup force [backup | primary]

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

backup	Force backup regardless of primary link state.
primary	Force primary link regardless of its state.

Default Values

By default, this feature is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to force this interface into dial-backup:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup force backup
```

dial-backup maximum-retry *<attempts>*

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

<attempts>	Selects the number of call retries that will be made after a link failure (valid range: 0 to 15). Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to 0 attempts.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to retry a dial-backup call four times before considering backup operation not available:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup maximum-retry 4
```

dial-backup number *<digits>* [analog | digital-56k | digital 64k] *<isdn min chan> <isdn max chan> <interface>*

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

<digits>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates number connects to an analog modem.
digital-56k	Indicates number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates number belongs to a digital 64 kbps per DS0 connection.
<isdn min chan>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection (Range: 1 to 24).
<isdn mas chan>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection (Range: 1 to 24).
<interface>	Specifies the PPP interface (e.g., PPP 3) to use when originating or answering using this number.

Default Values

By default, there are no configured dial-backup numbers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to dial 704-555-1212 (digital 64 kbps connection) to initiate dial-backup operation on this endpoint using interface PPP 3:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup number 7045551212 digital-64k 1 1 ppp 3
```

dial-backup priority *<value>*

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

<value>	Sets the relative priority of this link (valid range: 0 to 100). A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to 50.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example assigns the highest priority to this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup priority 100
```

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

No subcommands.

Default Values

By default, the AOS does not randomize the dial-backup call timers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to randomize the dial-backup timers associated with this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup randomize-timers
```

dial-backup redial-delay *<seconds>*

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

<seconds>	Specifies the delay in seconds between attempting to re-dial a failed backup attempt. Range: 10 to 3600.

Default Values

By default, **dial-backup redial-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures a redial delay of 25 seconds on this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup redial-delay 25
```

dial-backup restore-delay *<seconds>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is "bouncing" in and out of alarm. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

<seconds>	Specifies the number of seconds the AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range: 10 to 86,400.

Default Values

By default, **dial-backup restore-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 30 seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup restore-delay 30
```

dial-backup schedule [day | enable-time | disable-time]

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial-backup (as specified). For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 901.

Syntax Description

day	Sets the days to allow backup (valid range: Monday through Sunday).
enable-time	Sets the time of day to enable backup. Time is entered in 24-hour format (00:00).
disable-time	Sets the time of day to disable backup.

Default Values

By default, dial-backup is enabled for all days and times if the dial-backup auto-backup command has been issued and the dial-backup schedule has not been entered.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example enables dial-backup Monday through Friday 8:00 am to 7:00 pm:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup schedule enable-time 08:00
(config-ppp 1)#dial-backup schedule disable-time 19:00
(config-ppp 1)#no dial-backup schedule day Saturday
(config-ppp 1)#no dial-backup schedule day Sunday
```

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example deactivates the configured dial-backup interface:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup shutdown
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

Refer to *Functional Notes,* below, for argument descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A Web-based interface provides two levels of control over your domain, catering to average or power users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs, and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service, in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address doesn't change often or at all, but you still want an easy name to remember it by (without having to purchase your own domain name) Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com) you need Custom DNS service which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the **dynamic-dns** to **dyndns-custom** with hostname **host**, username **user**, and password **pass**:

```
(config)#interface ppp 1
(config-ppp1)#dynamic-dns dyndns-custom host user pass
```

fair-queue *<threshold>*

Use the **fair-queue** command to enable weighted fair queuing (WFQ) on an interface. Use the **no** form of this command to disable WFQ and enable FIFO queueing for an interface. WFQ is enabled by default for WAN interfaces.

Syntax Description

<threshold>	Optional. Specifies the maximum number of packets that can be present in each conversation sub-queue. Packets received for a conversation after this limit is reached are discarded. Range: 16 to 512 packets.

Default Values

By default, **fair-queue** is enabled with a threshold of 64 packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables WFQ on the interface with a threshold set at 100 packets:

```
(config)#interface ppp 1
(config-ppp 1)#fair-queue 100
```

hold-queue *<queue size>* out

Use the **hold-queue out** command to change the overall size of an interface's WAN output queue.

Syntax Description

<queue size>	Specifies the total number of packets the output queue can contain before packets are dropped. Range 16 to 1000.

Default Values

The default queue size for WFQ is 400. The default queue size for PPP FIFO and Frame Relay round-robin is 200.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example sets the overall output queue size to 700:

```
(config)#interface ppp 1
(config-ppp 1)#hold-queue 700 out
```

ip access-group *<listname>* [in | out]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Indicates the assigned IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the router to only allow Telnet traffic into the PPP interface:

```
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#interface ppp 1
(config-ppp 1)#ip access-group TelnetOnly in
```

ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface.

Syntax Description

No subcommands.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 8.1	Command expanded to include PPP interface.

Usage Examples

The following example enables DHCP operation on the PPP interface 1:

```
(config)#interface ppp 1
(config-ppp 1)#ip address dhcp
```

ip address negotiated [no-default]

Use the **ip address negotiated** command to allow the interface to negotiate (i.e., be assigned) an IP address from the far end PPP connection. Use the **no** form of this command to disable the negotiation for an IP address

Syntax Description

no-default	Optional. Prevents the insertion of a default route. Some systems already have a default route configured and need a static route to the PPP interface to function correctly.

Default Values

By default, the interface is assigned an address with the **ip address** *<address><mask>* command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example enables the PPP interface to negotiate an IP address from the far end connection:

```
(config)#interface ppp 1
(config-ppp 1)#ip address negotiated
```

The following example enables the PPP interface to negotiate an IP address from the far end connection without inserting a default route:

```
(config)#interface ppp 1
(config-ppp 1)#ip address negotiated no-default
```

ip address *<address> <mask>* secondary

Use the **ip address** command to define an IP address on the specified interface. Use the optional keyword **secondary** to define a secondary IP address. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<mask>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Configures a secondary IP address for the specified interface.

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use secondary IP addresses to allow dual subnets on a single interface (when you need more IP addresses than the primary subnet can provide). When using secondary IP addresses, avoid routing loops by verifying that all devices on the network segment are configured with secondary IP addresses on the secondary subnet.

Usage Examples

The following example configures a secondary IP address of **192.22.72.101/30**:

```
(config)#interface ppp 1
(config-ppp 1)#ip address 192.22.72.101 255.255.255.252 secondary
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The* ***ip helper*** *command must be used in conjunction with the* ***ip forward-protocol*** *command to configure the AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <port number>* on page 378 *for more information.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets.

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign a helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address 192.33.5.99:

```
(config)#ip forward-protocol udp domain
(config)#interface ppp 1
(config-ppp 1)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description	
immediate-leave	If only one host (or IGMP snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval <*milliseconds*>	Controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65535 ms. Default: 1000 ms.
querier-timeout <*seconds*>	Specifies the number of seconds that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range: 60 to 300 seconds. Default: 2x the **query-interval** value.
query-interval <*seconds* >	Specifies the interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65535 seconds. Default: 60 seconds.
query-max-response-time <*seconds*>	Specifies the maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group <*group-address*>	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface's IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
(config)#interface ppp 1
(config-ppp 1)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface and place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip mcast-stub downstream
```

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the IGMP proxy. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 10.1	Command was expanded to include PPP interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy.

Usage Examples

The following example sets the helper address as the IGMP proxy:

```
(config)#interface ppp 1
(config-ppp 1)#ip mcast-stub helper-enable
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key *<password>*	Assigns a simple-text authentication password to be used by other routers using the OSPF simple password authentication.
cost *<value>*	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 165,535.
dead-interval *<seconds>*	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range: 0 32,767.
hello-interval *<seconds>*	Specifies the interval between hello packets sent on the interface. Range: 0 32,767.
message-digest-key *<keyid>* **md5** *<key>*	Configures OSPF Message Digest 5 (MD5) authentication (16-byte max) keys.
priority *<value>*	Sets the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0 255.
retransmit-interval *<seconds>*	Specifies the time between link-state advertisements (LSAs). Range: 0 32,767.
transmit-delay *<seconds>*	Sets the estimated time required to send an LSA on the interface. Range: 0 32,767.

Default Values

retransmit-interval *<seconds>*	5 seconds
transmit-delay *<seconds>*	1 second
hello-interval *<seconds>*	10 seconds: Ethernet, point-to-point, Frame Relay, and PPP
dead-interval *<seconds>*	40 seconds

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Example

The following example sets the maximum number of seconds allowed between hello packets to 25,000:

```
(config)#interface ppp 1
(config-ppp 1)#ip ospf dead-interval 25000
```

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Selects message-digest authentication type.
null	Optional. Specifies that no authentication be used.

Default Values

By default, **ip ospf authentication** is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example specifies that no authentication will be used on the PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP and Frame Relay default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface ppp 1
(config-ppp 1)#ip ospf network broadcast
```

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM Sparse Mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip pim sparse-mode
```

ip pim-sparse dr-priority *<priority number>*

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the routers priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<priority number>	Specifies the priority number for the DR router. Valid range is 1 to 4,294,967,295.

Default Values

By default, the DR priority is set to 1.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the DR priority to 5:

```
(config)#interface ppp 1
(config-ppp 1)#ip pim-sparse dr-priority 5
```

ip pim-sparse hello-timer *<time>*

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time in seconds between hello transmissions. Valid range is 10 to 12,600 seconds.

Default Values

By default, the hello timer is set to 30 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the hello timer to 60 seconds:

```
(config)#interface ppp 1
(config-ppp 1)#ip pim-sparse hello-timer 60
```

ip pim-sparse nbr-timeout *<time>*

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is 30 to 10,800 seconds.

Default Values

By default, the nbr-timeout is set to 105 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

```
(config)#interface ppp 1
(config-ppp 1)#ip pim-sparse nbr-timeout 300
```

ip pim-sparse override-interval *<time>*

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the LAN may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the delay time in milliseconds. Valid range is 0 to 65,535 milliseconds.

Default Values

By default, the override-interval is set to 2500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override-interval to 3000 milliseconds:

```
(config)#interface ppp 1
(config-ppp 1)#ip pim-sparse override-interval 3000
```

ip pim-sparse propagation-delay *<time>*

Use the **ip pim-sparse propagation-delay** command to specify protocol-independent multicast (PIM) sparse join/prune propagation delay. This is the expected propagation delay in milliseconds over the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the expected propagation delay in milliseconds. Valid range is 0 to 32,767 milliseconds.

Default Values

By default, the propagation-delay is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation-delay to 1000 milliseconds:

```
(config)#interface ppp 1
(config-ppp 1)#ip pim-sparse propagation-delay 1000
```

ip policy route-map *<policy name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<policy name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip policy route-map policy1
```

ip proxy-arp *<address> <subnet mask>*

Use the **ip proxy-arp** to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example, 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy ARP is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, the AOS will respond to all proxy ARP requests with its specified MAC address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following enables proxy ARP on the virtual PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Accepts only received RIP version 1 packets on the interface.
2	Accepts only received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

The AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual PPP interface to accept only RIP version 2 packets:

```
(config)#interface ppp 1
(config-ppp 1)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Transmits only RIP version 1 packets on the interface.
2	Transmits only RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Use the **ip rip send version** to specify a RIP version that overrides the **version** (in the Router RIP) configuration.

The AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the virtual PPP interface to transmit only RIP version 2 packets:

```
(config)#interface ppp 1
(config-ppp 1)#ip rip send version 2
```

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route cache is enabled for all virtual PPP interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

Fast-cache switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast-cache switching on the virtual PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#ip route-cache
```

ip unnumbered *<interface>*

Use the **ip unnumbered** command to use the IP address assigned to the specified interface for all IP processing on the active interface. Use the **no** form of this command to remove the unnumbered configuration.

Syntax Description

<interface>	Specifies the interface (in the format **type slot/port**) that contains the IP address to use as the source address for all packets transmitted on this interface.

Default Values

By default, all interfaces are configured to use a specified IP address (using the **ip address** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 11.1	Command was expanded to include demand interfaces.

Functional Notes

If **ip unnumbered** is enabled on an interface, all IP traffic from the interface will use a source IP address taken from the specified interface. For example, specifying **ip unnumbered eth 0/1** while in the PPP Interface Configuration mode configures the PPP interface to use the IP address assigned to the Ethernet interface for all IP processing. In addition, the AOS uses the specified interface information when sending route updates over the unnumbered interface. Static routes may either use the interface name (ppp 1) or the far-end address (if it will be discovered).

Usage Examples

The following example configures the PPP interface (labeled **ppp 1**) to use the IP address assigned to the Ethernet interface (**eth 0/1**):

```
(config)#interface ppp 1
(config-ppp 1)#ip unnumbered eth 0/1
```

keepalive *<seconds>*

Use the **keepalive** command to enable the transmission of keepalive packets on the interface and specify the time interval in seconds between transmitted packets.

Syntax Description

<seconds>	Defines the time interval (in seconds) between transmitted keepalive packets (valid range: 0 to 32,767 seconds).

Default Values

By default, the time interval between transmitted keepalive packets is 10 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

If three keepalive packets are sent to an interface with no response, the interface is considered down. To detect interface failures quickly, specify a smaller keepalive time.

Usage Examples

The following example specifies a keepalive time of 5 seconds on the virtual PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#keepalive 5
```

lldp receive

Use the **lldp receive** command to allow LLDP packets to be received on this interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the PPP interface to receive LLDP packets:

```
(config)#interface ppp 1
(config-ppp 1)#lldp receive
```

lldp send [management-address | port-description | system-capabilities | system-description | system-name | and-receive]

Use the **lldp send** command to configure this interface to transmit LLDP packets or to control the types of information contained in the LLDP packets transmitted by this interface.

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device's system capabilities on this interface.
system-description	Enables transmission of this device's system description on this interface.
system-name	Enables transmission of this device's system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

Be default, all interfaces are configured to transmit and receive LLDP packets of all types.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the PPP interface to transmit LLDP packets containing all enabled information types:

```
(config)#interface ppp 1
(config-ppp 1)#lldp send
```

The following example configures the PPP interface to transmit and receive LLDP packets containing all information types:

```
(config)#interface ppp 1
(config-ppp 1)#lldp send and-receive
```

max-reserved-bandwidth *<percent>*

Use the **max-reserved-bandwidth** command to define the maximum amount of interface bandwidth reserved for Quality of Service (QoS). Use the **no** form of this command to return to the default value.

Syntax Description

<percent>	Specifies the maximum amount of bandwidth to reserve for QoS. This setting is configured as a percentage of the total interface speed. Range: 1 to 100 percent.

Default Values

By default, **max-reserved-bandwidth** is set to 75 percent.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the **reserved-bandwidth** maximum at 80 percent:

```
(config)#interface ppp 1
(config-ppp 1)#max-reserved-bandwidth 80
```

mtu *<size>*

Use the **mtu** command to configure the maximum transmit unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size>	Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:	
	ATM interfaces	64 to 1520
	Demand interfaces	64 to 1520
	Ethernet interfaces	64 to 1500
	FDL interfaces	64 to 256
	HDLC interfaces	64 to 1520
	Loopback interfaces	64 to 1500
	Tunnel interfaces	64 to 18,190
	Virtual Frame Relay sub-interfaces	64 to 1520
	Virtual PPP interfaces	64 to 1500

Default Values

<size>	The default values for the various interfaces are listed below:	
	ATM interfaces	1500
	Demand interfaces	1500
	Ethernet interfaces	1500
	FDL interfaces	256
	HDLC interfaces	1500
	Loopback interfaces	1500
	Tunnel interfaces	1500
	Virtual Frame Relay sub-interfaces	1500
	Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the virtual PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#mtu 1200
```

peer default ip address *<address>*

Use the **peer default ip address** command to specify the default IP address of the remote end of this interface.

Syntax Description

<address>	Specifies the default IP address for the remote end (A.B.C.D).

Default Values

By default, there is no assigned peer default IP address.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

This command is useful if the peer does not send the IP address option during PPP negotiations.

Usage Examples

The following example sets the default peer IP address to 192.22.71.50:

```
(config)#interface ppp 1
(config-ppp 1)#peer default ip address 192.22.71.50
```

ppp authentication [chap | pap]

Use the **ppp authentication** command to specify the authentication protocol on the PPP virtual interface that the peer should use to authenticate itself.

Syntax Description

chap	Configures CHAP authentication on the interface.
pap	Configures PAP authentication on the interface.

Default Values

By default, PPP endpoints have no authentication configured.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.

Technology Review

CHAP and PAP are two authentication methods that enjoy widespread support. Both methods are included in the AOS and are easily configured.

> NOTE *The authentication method set up on the local router can be different from that on the peer. Also, just because one router requires authentication from its peer does not mean it also has to authenticate itself to the peer.*

Defining PAP

The Password Authentication Protocol (PAP) is used to verify that the PPP peer is a permitted device by checking a username and password configured on the peer. The username and password are both sent unencrypted across the connecting private circuit.

PAP requires two-way message passing. First, the router that is required to be authenticated (say the peer) sends an authentication request with its username and password to the router requiring authentication (say the local router). The local router then looks up the username and password in the username database within the PPP interface, and if they match sends an authentication acknowledge back to the peer.

> NOTE *The PPP username and password database is separate and distinct from the global username password database. For PAP and CHAP, use the database under the PPP interface configuration.*

Several example scenarios are given below for clarity.

Configuring PAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication pap
Local(config-ppp 1)#username farend password far
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp pap sent-username farend password far
```

The first line of the configuration sets the authentication mode as PAP. This means the peer is required to authenticate itself to the local router via PAP. The second line is the username and password expected to be sent from the peer. On the peer, the **ppp pap sent-username** command is used to specify the appropriate matching username and password.

Configuring PAP Example 2: Both routers require the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication pap
Local(config-ppp 1)#username farend password far
Local(config-ppp 1)#ppp pap sent-username nearend password near
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp authentication pap
Peer(config-ppp 1)#username nearend password near
Peer(config-ppp 1)#ppp pap sent-username farend password far
```

Now both routers send the authentication request, verify that the username and password sent match what is expected in the database, and send an authentication acknowledge.

Defining CHAP

The Challenge-Handshake Authentication Protocol (CHAP) is a three-way authentication protocol composed of a challenge response and success or failure. The MD5 protocol is used to protect usernames and passwords in the response.

First, the local router (requiring its peer to be authenticated) sends a "challenge" containing the unencrypted username of the peer and a random number. The username of the peer is found in the username database within the PPP interface of the local router. The peer then looks up the username in the username database within the PPP interface, and if found takes the corresponding password and its own hostname and sends a "response" back to the local router. This data is encrypted. The local router verifies that the username and password are in its own username database within the PPP interface, and if so sends a "success" back to the peer.

> NOTE *The PPP username and password database is separate and distinct from the global username password database. For PAP and CHAP, use the database under the PPP interface configuration.*

Several example scenarios are given below for clarity.

Configuring CHAP Example 1: Only the local router requires the peer to authenticate itself.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication chap
Local(config-ppp 1)#username Peer password same
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp chap password same
```

The first line of this configuration sets the authentication mode to CHAP. This means the peer is required to authenticate itself to the local router via CHAP. The second line is the username and password expected to be sent from the peer. The peer uses its **hostname** and **ppp chap password** commands to send the proper authentication information.

> NOTE *Both ends must have identical passwords.*

Configuring CHAP Example 2: Using the ppp chap hostname command as an alternate solution.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication chap
Local(config-ppp 1)#username farend password same
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp chap hostname farend
Peer(config-ppp 1)#ppp chap password same
```

Notice the local router is expecting username "farend" even though the peer router's hostname is "Peer." Therefore the peer router can use the **ppp chap hostname** command to send the correct name in the challenge.

> NOTE *Both ends must have identical passwords.*

Configuring CHAP Example 3: Both routers require each other to authenticate themselves using the same shared password.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication chap
Local(config-ppp 1)#username Peer password same
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp authentication chap
Peer(config-ppp 1)#username Local password same
```

This is basically identical to Example 1 except that both routers will now challenge each other and respond.

> *Both ends must have identical passwords.*

Configuring CHAP Example 4: Both routers require each other to authenticate themselves using two separate shared passwords.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication chap
Local(config-ppp 1)#username Peer password far
Local(config-ppp 1)#ppp chap password near
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp authentication chap
Peer(config-ppp 1)#username Local password near
Peer(config-ppp 1)#ppp chap password far
```

This is basically identical to Example 3, except that there are two separate shared passwords.

> *Notice this example has both ends using different sets of passwords.*

Configuring CHAP Example 5: Using the ppp chap hostname command as an alternate solution.

On the local router (hostname Local):

```
Local(config-ppp 1)#ppp authentication chap
Local(config-ppp 1)#username farend password far
Local(config-ppp 1)#ppp chap hostname nearend
Local(config-ppp 1)#ppp chap password near
```

On the peer (hostname Peer):

```
Peer(config-ppp 1)#ppp authentication chap
Peer(config-ppp 1)#username nearend password near
Peer(config-ppp 1)#ppp chap hostname farend
Peer(config-ppp 1)#ppp chap password far
```

Notice the local router is expecting username "farend" even though the peer router's hostname is "Peer." Therefore the peer router can use the **ppp chap hostname** command to send the correct name on the challenge.

NOTE *Notice this example has both ends using different sets of passwords.*

ppp chap hostname *<hostname>*

Use the **ppp chap hostname** command to configure an alternate hostname for CHAP PPP authentication. Use the **no** form of this command to remove a configured hostname. For more information on PAP and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication [chap | pap]* on page 952.

Syntax Description

<hostname>	Specifies a hostname using an alphanumeric string up to 80 characters in length.

Default Values

By default, there are no configured PPP CHAP hostnames.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a PPP CHAP hostname of **my_host**:

```
(config)#interface ppp 1
(config-ppp 1)#ppp chap hostname my_host
```

ppp chap password *<password>*

Use the **ppp chap password** command to configure an alternate password when the peer requires CHAP PPP authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication [chap | pap]* on page 952.

Syntax Description

<password>	Specifies a password using an alphanumeric string up to 80 characters in length.

Default Values

By default, there is no defined PPP CHAP password.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a PPP CHAP password of **my_password**:

```
(config)#interface ppp 1
(config-ppp 1)#ppp chap password my_password
```

ppp multilink [fragmentation | interleave]

Use the **ppp multilink** command to enable multilink PPP (MPPP) operation om an existing PPP interface. Use the **no** form of this command to disable.

Syntax Description

fragmentation	Enables multilink fragmentation operation.
interleave	Enables multilink interleave operation.

Default Values

By default, MPPP is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 7.2	Fragmentation and interleave operation were added.

Functional Notes

When enabled, this interface is capable of the following:

- Combining multiple physical links into one logical link.
- Receiving upper layer protocol data units (PDU), fragmenting and transmitting over the physical links.
- Receiving fragments over the physical links and reassembling them into PDUs.

The fragmentation and interleave options can be used to enhance the multilink operation. Fragmentation is used to reduce serialization delays of large packets. The fragmentation process evenly divides the data among all links in the bundle with a minimum packet size of 96 bytes. The interleave operation is used with streaming protocols to reduce delay by giving priority to packets identified as high priority. In order delivery is guaranteed with multilink fragmentation, but is not guaranteed with multilink interleave operation.

The multilink bundle will remain active with a minimum of one physical link. Physical links may be dynamically added or removed from the multilink bundle with minor interruption to traffic flow.

Usage Examples

The following example enables MPPP:

```
(config)#interface ppp 1
(config-ppp 1)#ppp multilink
```

ppp pap sent-username *<username>* password *<password>*

Use the **ppp pap sent-username/password** command to configure a username and password when the peer requires PAP PPP authentication. Use the **no** form of this command to remove a configured password. For more information on PAP and CHAP functionality, refer to the *Technology Review* section for the command *ppp authentication [chap | pap]* on page 952.

Syntax Description

<username>	Specifies a username by alphanumeric string up to 80 characters in length (the username is case-sensitive).
<password>	Specifies a password by alphanumeric string up to 80 characters in length (the password is case-sensitive).

Default Values

By default, there is no defined **ppp pap sent-username** and **password**.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies a PPP PAP sent-username of **local** and a password of **my_password**:

```
(config)#interface ppp 1
(config-ppp 1)#ppp pap sent-username local password my_password
```

pppoe ac-name *<name>*

Use the **pppoe ac-name** command to identify the Access Concentrator (AC) with which the AOS expects to establish a PPPoE session. Use the **no** form of this command to return to the default setting.

Syntax Description

<name>	Specifies an AC by text string (up to 255 characters) corresponding to the AC-Name Tag under RFC2516. If this field is not specified, any access concentrator is acceptable. The AC value may be a combination of trademark, model, and serial ID information (or simply the MAC address of the unit).

Default Values

By default, no AC is specified.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example identifies the AC with which the AOS expects to establish a PPPoE session:

```
(config)#interface ppp 1
(config-ppp 1)#pppoe acc-name Access_Concentrator_Name
```

pppoe service-name *<name>*

Use the **pppoe service-name** command to use this tag value to filter PPPoE session offers from PPPoE servers. Use the **no** form of this command to return to the default setting.

Syntax Description

<name>	Specifies a service name by text string (up to 255 characters) corresponding to the Service-Name Tags under RFC2516. This string indicates an ISP name (or a class or quality of service). If this field is not specified, any service is acceptable.

Default Values

By default, no names are specified.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example defines a service type that is not to be accepted by the AOS:

```
(config)#interface ppp 1
(config-ppp 1)#pppoe service-name Service_Name
```

qos-policy out *<mapname>*

Use the **qos-policy out** command to apply a previously-configured QoS map to an interface. Use the **no** form of this command to remove the map from the interface. The keyword **out** specifies that this policy will be applied to outgoing packets.

Syntax Description

<mapname>	Specifies the name of a previously-created QoS map (refer to *qos map <mapname> <sequence number>* on page 434 for more information).

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Functional Notes

When a QoS policy is applied to an interface, it may be disabled if the interface bandwidth is not adequate to support the requested bandwidth on the map set. Once the bandwidth problem is resolved, the map will work again. The bandwidth will be rechecked on any of the following changes:

1. A priority or class-based entry is added to, deleted from, or changed in a QoS map set.
2. The interface bandwidth is changed by the **bandwidth** command on the interface.
3. A QoS policy is applied to an interface.
4. A cross-connect is created that includes an interface with a QoS policy.
5. The interface queuing method is changed to fair-queue to use weighted fair queuing.
6. The interface operational status changes.
7. The interface bandwidth changes for other reasons (e.g., when ADSL finishes training).

In order to prevent the map from being disabled in cases of temporary inadequate bandwidth (e.g., a single link goes down in a dual T1 multilink configuration where the map requests more than one T1's worth of bandwidth), the QoS map uses the maximum theoretical bandwidth on an interface, not the actual bandwidth at that time. This actually helps QoS keep higher priority class-based traffic working better than best-effort traffic when the bandwidth drops.

Usage Examples

The following example applies the QoS map **VOICEMAP** to the PPP 1 interface:

```
(config)#interface ppp 1
(config-ppp 1)#qos-policy out VOICEMAP
```

snmp trap link-status

Use the **snmp trap link-status** command to control the Simple Network Management Protocol (SNMP) variable ifLinkUpDownTrapEnable (RFC2863) to enable (or disable) the interface to send SNMP traps when there is an interface status change. Use the **no** form of this command to disable this trap.

Syntax Description

No subcommands.

Default Values

By default, the ifLinkUpDownTrapEnable OID is enabled for all interfaces except virtual Frame Relay interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 3.1	Command was extended to the SHDSL interface.
Release 5.1	Command was expanded to include Gigabit Ethernet, port channel, VLAN, E1, and G.703 interfaces.

Functional Notes

The **snmp trap link-status** command is used to control the RFC2863 ifLinkUpDownTrapEnable OID (OID number 1.3.6.1.2.1.31.1.1.1.14.0).

Usage Examples

The following example disables the link-status trap on the virtual PPP interface:

```
(config)#interface ppp 1
(config-ppp 1)#no snmp trap link-status
```

username *<username>* password *<password>*

Configures the username and password of the peer to use for PPP authentication.

Syntax Description

<username>	Specifies a username by alphanumerical string up to 30 characters in length (the username is case-sensitive).
<password>	Specifies a password by alphanumerical string up to 30 characters in length (the password is case-sensitive).

Default Values

By default, there is no established username and password.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

PAP uses this entry to check received information from the peer. CHAP uses this entry to check the received peer hostname and a common password.

Usage Examples

The following example creates a username of **ADTRAN** with password **ADTRAN** for the PPP link labeled 5:

```
(config)#interface ppp 5
(config-ppp 5)#username ADTRAN password ADTRAN
```

TUNNEL CONFIGURATION COMMAND SET

To activate the Tunnel Configuration mode, enter the **interface tunnel** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface tunnel 1
(config-tunnel 1)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

alias <"text"> on page 27

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-policy <policyname> on page 968

bandwidth <value> on page 971

crypto map <mapname> on page 972

dial-backup commands begin on page 974

dynamic-dns [dyndns | dyndns-custom | dyndns-static] <hostname> <username> <password> on page 990

ip commands begin on page 992

keepalive <period> <retries> on page 1016

lldp receive on page 1017

lldp send [management-address l port-description l system-capabilities l system-description l system-name l and-receive] on page 1018

mtu <size> on page 1020

tunnel checksum on page 1021

tunnel destination <ip address> on page 1022

tunnel key <value> on page 1023

tunnel mode gre on page 1024

tunnel sequence-datagrams on page 1025

tunnel source [<ip address> | <interface>] on page 1026

access-policy *<policyname>*

Use the **access-policy** command to assign a specified access policy for the inbound traffic on an interface. Use the **no** form of this command to remove an access policy association.

> *Configured access policies will only be active if the* ***ip firewall*** *command has been entered at the Global Configuration mode prompt to enable the AOS security features. All configuration parameters are valid, but no security data processing will be attempted unless the security features are enabled.*

Syntax Description

<policyname>	Identifies the configured access policy by alphanumeric descriptor (all access policy descriptors are case-sensitive).

Default Values

By default, there are no configured access policies associated with an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access-policy** *<policy name>*.

Usage Examples

The following example associates the access policy **UnTrusted** (to allow inbound traffic to the Web server) to the tunnel 1 interface:

Enable the AOS security features:

```
(config)#ip firewall
```

Create the access list (this is the packet selector):

```
(config)#ip access-list extended InWeb
(config-ext-nacl)#permit tcp any host 63.12.5.253 eq 80
```

Create the access policy that contains the access list **InWeb**:

```
(config)#ip policy-class UnTrusted
(config-policy-class)#allow list InWeb
```

Associate the access policy with the tunnel 1 interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#access-policy UnTrusted
```

Technology Review

Creating access policies and lists to regulate traffic through the routed network is a four-step process:

Step 1:

Enable the security features of the AOS using the **ip firewall** command.

Step 2:

Create an access list to permit or deny specified traffic. Standard access lists provide pattern matching for source IP addresses only. (Use extended access lists for more flexible pattern matching.) IP addresses can be expressed in one of three ways:

1. Using the keyword **any** to match any IP address. For example, entering **deny any** will effectively shut down the interface that uses the access list because all traffic will match the **any** keyword.
2. Using the **host** <*A.B.C.D*> to specify a single host address. For example, entering **permit host 196.173.22.253** will allow all traffic from the host with an IP address of 196.173.22.253.
3. Using the <*A.B.C.D*> <*wildcard*> format to match all IP addresses in a "range." Wildcard masks work in reverse logic from subnet mask. Specifying a one in the wildcard mask equates to a "don't care." For example, entering **permit 192.168.0.0 0.0.0.255** will permit all traffic from the 192.168.0.0/24 network.

Step 3:

Create an IP policy class that uses a configured access list. AOS access policies are used to permit, deny, or manipulate (using **NAT**) data for each physical interface. Each ACP consists of a selector (**access list**) and an action (**allow**, **discard**, **NAT**). When packets are received on an interface, the configured ACPs are applied to determine whether the data will be processed or discarded. Possible actions performed by the access policy are as follows:

allow list <*access list names*>

All packets passed by the access list(s) entered will be allowed to enter the router system.

discard list <*access list names*>

All packets passed by the access list(s) entered will be dropped from the router system.

allow list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be permitted to enter the router system. This allows for configurations to permit packets to a single interface and not the entire system.

discard list <*access list names*> **policy** <*access policy name*>

All packets passed by the access list(s) entered and destined for the interface using the access policy listed will be blocked from the router system. This allows for configurations to deny packets on a specified interface.

nat source list <*access list names*> **address** <*IP address*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the entered IP address. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address entered. This hides private IP addresses from outside the local network.

nat source list <*access list names*> **interface** <*interface*> **overload**

All packets passed by the access list(s) entered will be modified to replace the source IP address with the primary IP address of the listed interface. The **overload** keyword allows multiple source IP addresses to be replaced with the single IP address of the specified interface. This hides private IP addresses from outside the local network.

nat destination list <*access list names*> **address** <*IP address*>

All packets passed by the access list(s) entered will be modified to replace the destination IP address with the entered IP address. The **overload** keyword is not an option when performing NAT on the destination IP address; each private address must have a unique public address. This hides private IP addresses from outside the local network.

Step 4:

Apply the created access policy to an interface. To assign an access policy to an interface, enter the interface configuration mode for the desired interface and enter **access policy** <*policy name*>. The following example assigns access policy **MatchAll** to the tunnel 1 interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#access-policy MatchAll
```

bandwidth *<value>*

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

<value>	Specifies bandwidth in kbps.

Default Values

To view default values, use the **show interfaces** command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 5.1	Command was expanded to include Ethernet sub-interfaces.
Release 6.1	Command was expanded to include VLAN interfaces.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

The **bandwidth** command is an informational value that is communicated to the higher-level protocols to be used in cost calculations. This is a routing parameter only and does not affect the physical interface.

Usage Examples

The following example sets bandwidth of the tunnel 1 interface to 10 Mbps:

```
(config)#interface tunnel 1
(config-tunnel 1)#bandwidth 10000
```

crypto map *<mapname>*

Use the **crypto map** command to associate crypto maps with the interface.

> NOTE *When you apply a map to an interface, you are applying all crypto maps with the given map name. This allows you to apply multiple crypto maps if you have created maps which share the same name but have different map index numbers.*

> NOTE *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

Syntax Description

<mapname>	Assigns a crypto map name to the interface.

Default Values

By default, no crypto maps are assigned to an interface.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

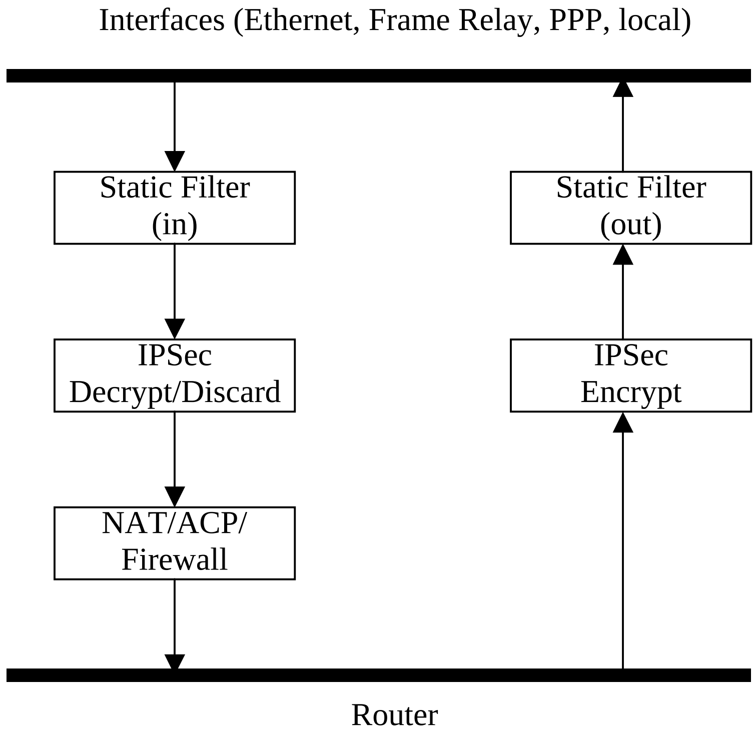
Command History

Release 4.1	Command was introduced.

Functional Notes

When configuring a system to use both the stateful inspection firewall and IKE negotiation for VPN, keep the following notes in mind.

When defining the policy class and associated access-control lists (ACLs) that describe the behavior of the firewall, do not forget to include the traffic coming into the system over a VPN tunnel terminated by the system. The firewall should be set up with respect to the unencrypted traffic that is destined to be sent or received over the VPN tunnel. The following diagram represents typical AOS data-flow logic.



As shown in the diagram above, data coming into the product is first processed by the static filter associated with the interface on which the data is received. This access group is a true static filter and is available for use regardless of whether the firewall is enabled or disabled. Next (if the data is encrypted) it is sent to the IPSec engine for decryption. The decrypted data is then processed by the stateful inspection firewall. Therefore, given a terminating VPN tunnel, only unencrypted data is processed by the firewall.

The ACLs for a crypto map on an interface work in reverse logic to the ACLs for a policy class on an interface. When specifying the ACLs for a crypto map, the source information is the private local-side, unencrypted source of the data. The destination information will be the far end, unencrypted destination of the data. However, ACLs for a policy class work in reverse. The source information for the ACL in a policy class is the far end. The destination information is the local side.

Usage Examples

The following example applies all crypto maps with the name **MyMap** to the tunnel interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#crypto map MyMap
```

dial-backup auto-backup

Use the **dial-backup auto-backup** command to configure the PPP interface to automatically attempt a dial-backup upon failure. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically attempt dial-backup upon a failure.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example enables automatic dial-backup on the endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup auto-backup
```

dial-backup auto-restore

Use the **dial-backup auto-restore** command to configure the interface to automatically discontinue dial-backup when all network conditions are operational. Use the **no** form of this command to disable the auto-restore feature. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

No subcommands.

Default Values

By default, all backup endpoints will automatically restore the primary connection when the failure condition clears.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to automatically restore the primary connection when the failure condition clears:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup auto-restore
```

dial-backup backup-delay *<seconds>*

Use the **dial-backup backup-delay** command to configure the amount of time the router will wait after the failure condition is recognized before attempting to backup the link. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

<seconds>	Specifies the delay period (in seconds) a failure must be active before the AOS will enter backup operation on the interface. Range: 10 to 86,400 seconds.

Default Values

By default, the **dial-backup backup-delay** period is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 60 seconds (on an endpoint with an active alarm condition) before attempting dial-backup operation:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup backup-delay 60
```

dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]

Use the **dial-backup call-mode** command to combine user data with pattern data to ensure data does not mirror standard DDS loop codes (use only on 64 kbps circuits without Frame Relay signaling). Use the **no** form of this command to return to the default value.

Syntax Description

answer	Answers and backs up primary link on failure.
answer-always	Answers and backs up regardless of primary link state.
originate	Originates backup call on primary link failure.
originate-answer	Originates or answers call on primary link failure.
originate-answer-always	Originates on failure; answers and backs up always.

Default Values

By default, the **dial-backup call-mode** is set to **originate-answer.**

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Functional Notes

The majority of the configuration for PPP dial-backup is configured in the PPP interface's. However, the numbers dialed are configured in the primary interface. Full sample configurations follow:

Sample configuration for remote router (dialing out)

```
hostname "Remote3200"
enable password adtran
!
interface eth 0/1
  ip address  192.168.1.254  255.255.255.0
  no shutdown
!
interface modem 1/3
no shutdown
!
```

```
interface t1 1/1
coding b8zs
framing esf
clock source line
tdm-group 1 timeslots 1-24
no shutdown
!
interface ppp 1
ip address 10.1.1.2 255.255.255.252
dial-backup call-mode originate
dial-backup number 5551111 analog ppp 2
cross-connect 1 t1 1/1 1 ppp 1
!
interface ppp 2
description connected to corp for dial-backup
ip address 10.10.10.2 255.255.255.252
ppp authentication pap
ppp pap sent-username joe password pswrd
!
ip route 0.0.0.0  0.0.0.0  10.1.1.1
!
line telnet 0 4
password adtran
```

Sample configuration for central router (dialing in)

```
hostname "Central3200"
enable password adtran
!
interface eth 0/1
ip address  192.168.100.254  255.255.255.0
no shutdown
!
interface modem 1/3
no shutdown
!
interface t1 1/1
coding b8zs
framing esf
clock source line
tdm-group 1 timeslots 1-24
no shutdown
!
interface ppp 1
```

```
no shutdown
cross-connect 1 t1 1/1 1 ppp 1
ip address 10.1.1.1 255.255.255.252
dial-backup call-mode answer
dial-backup number 555-8888 analog ppp 2
!
interface ppp 2
description connection for remote 3200 dialin for backup
ip address 10.10.10.1 255.255.255.252
ppp authentication pap
username joe password pswrd
!
line telnet 0 4
password adtran
```

Usage Examples

The following example configures the AOS to answer dial-backup calls on this endpoint but never generate calls:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup call-mode answer-always
```

Technology Review

This technology review provides information regarding specific dial-backup router behavior (i.e., when the router will perform dial-backup, where in the configuration the AOS accesses specific routing information, etc.):

Dialing Out

1. The AOS determines to place an outbound call when either the Layer 1 or Layer 2 has a failure.
2. When placing outbound calls, the AOS matches the number dialed to a PPP interface. This is accomplished with an addition to the **dial-backup number** command (refer to *dial-backup number <digits> [analog | digital-56k | digital 64k] <isdn min chan> <isdn max chan> <interface>* on page 983).
3. When placing the call, the AOS uses the configuration of the related PPP interface for authentication and IP negotiation.
4. If the call fails to connect on the first number dialed, the AOS places a call to the second number if configured. The second number to be dialed references a separate PPP interface.

Dialing In

1. The AOS receives an inbound call on a physical interface.
2. Caller ID is used to match the **dial-backup number** command to the configured PPP interface.
3. If a match is found, the call connects and the AOS pulls down the primary connection if it is not already in a down state.
4. If no match is found from Caller ID, the call is terminated.

dial-backup connect-timeout *<seconds>*

Use the **dial-backup connect-timeout** command to specify the number of seconds to wait for a connection after a call is attempted before trying to call again or dialing a different number. It is recommended this number be greater than 60. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

<seconds>	Selects the amount of time (in seconds) that the router will wait for a connection before attempting another call (valid range: 10 to 300).

Default Values

By default, the **dial-backup connect-timeout** period is set to 60 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 120 seconds before retrying a failed dial-backup call:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup connect-timeout 120
```

dial-backup force [backup | primary]

Use the **dial-backup force** command to manually override the automatic dial-backup feature. This can be used to force a link into backup to allow maintenance to be performed on the primary link without disrupting data. Use the **no** form of this command to return to the normal dial-backup operation state. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

backup	Force backup regardless of primary link state.
primary	Force primary link regardless of its state.

Default Values

By default, this feature is disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to force this interface into dial-backup:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup force backup
```

dial-backup maximum-retry *<attempts>*

Use the **dial-backup maximum-retry** command to select the number of calls the router will make when attempting to backup a link. Use the **no** form of this command to return to the default state. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

<attempts>	Selects the number of call retries that will be made after a link failure (valid range: 0 to 15). Setting this value to 0 will allow unlimited retries during the time the network is failed.

Default Values

By default, **dial-backup maximum-retry** is set to 0 attempts.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to retry a dial-backup call four times before considering backup operation not available:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup maximum-retry 4
```

dial-backup number *<digits>* [analog | digital-56k | digital 64k] *<isdn min chan> <isdn max chan> <interface>*

Use the **dial-backup number** command to configure the phone number and the call type the router will dial upon network failure. Multiple entries can be made for an interface to allow alternate sites to be dialed. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

<digits>	Specifies the phone numbers to call when the backup is initiated.
analog	Indicates number connects to an analog modem.
digital-56k	Indicates number belongs to a digital 56 kbps per DS0 connection.
digital-64k	Indicates number belongs to a digital 64 kbps per DS0 connection.
<isdn min chan>	Specifies the minimum number of DS0s required for a digital 56 or 64 kbps connection (Range: 1 to 24).
<isdn mas chan>	Specifies the maximum number of DS0s desired for a digital 56 or 64 kbps connection (Range: 1 to 24).
<interface>	Specifies the PPP interface (e.g., PPP 3) to use when originating or answering using this number.

Default Values

By default, there are no configured dial-backup numbers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to dial 704-555-1212 (digital 64 kbps connection) to initiate dial-backup operation on this endpoint using interface PPP 3:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup number 7045551212 digital-64k 1 1 ppp 3
```

dial-backup priority *<value>*

Use the **dial-backup priority** command to select the backup priority for this interface. This allows the user to establish the highest priority backup link and ensure that link will override backups attempted by lower priority links. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

<value>	Sets the relative priority of this link (valid range: 0 to 100). A value of 100 designates the highest priority.

Default Values

By default, **dial-backup priority** is set to 50.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example assigns the highest priority to this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup priority 100
```

dial-backup randomize-timers

Use the **dial-backup randomize-timers** command to randomize the call timers to minimize potential contention for resources. Use the **no** form of this command to return to the default value. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

No subcommands.

Default Values

By default, the AOS does not randomize the dial-backup call timers.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to randomize the dial-backup timers associated with this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup randomize-timers
```

dial-backup redial-delay *<seconds>*

Use the **dial-backup redial-delay** command to configure the delay after an unsuccessful call until the call will be re-tried. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

<seconds>	Specifies the delay in seconds between attempting to re-dial a failed backup attempt. Range: 10 to 3600.

Default Values

By default, **dial-backup redial-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures a redial delay of 25 seconds on this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup redial-delay 25
```

dial-backup restore-delay *<seconds>*

Use the **dial-backup restore-delay** command to configure the amount of time the router will wait after the network is restored before disconnecting the backup link and reverting to the primary. This setting is used to prevent disconnecting the backup link if the primary link is "bouncing" in and out of alarm. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

<seconds>	Specifies the number of seconds the AOS will wait (after a primary link is restored) before disconnecting dial-backup operation. Range: 10 to 86,400.

Default Values

By default, **dial-backup restore-delay** is set to 10 seconds.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example configures the AOS to wait 30 seconds before disconnecting dial-backup operation and restoring the primary connection for this endpoint:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup restore-delay 30
```

dial-backup schedule [day | enable-time | disable-time]

Use the **dial-backup schedule** command to set the time of day that backup will be enabled. Use this command if backup is desired only during normal business hours and on specific days of the week. Use the **no** form of this command to disable dial-backup (as specified). For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command *dial-backup call-mode [answer | answer-always | originate | originate-answer | originate-answer-always]* on page 977.

Syntax Description

day	Sets the days to allow backup (valid range: Monday through Sunday).
enable-time	Sets the time of day to enable backup. Time is entered in 24-hour format (00:00).
disable-time	Sets the time of day to disable backup.

Default Values

By default, dial-backup is enabled for all days and times if the dial-backup auto-backup command has been issued and the dial-backup schedule has not been entered.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example enables dial-backup Monday through Friday 8:00 am to 7:00 pm:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup schedule enable-time 08:00
(config-ppp 1)#dial-backup schedule disable-time 19:00
(config-ppp 1)#no dial-backup schedule day Saturday
(config-ppp 1)#no dial-backup schedule day Sunday
```

dial-backup shutdown

Use the **dial-backup shutdown** command to deactivate all dial-backup functionality in the unit. Dial-backup configuration parameters are kept intact, but the unit will not initiate (or respond) to dial-backup sequences in the event of a network outage. Use the **no** form of this command to reactivate the dial-backup interface. For more detailed information on PPP dial-backup functionality, refer to the *Functional Notes* and *Technology Review* sections of the command.

Syntax Description

No subcommands.

Default Values

By default, all AOS interfaces are disabled.

Applicable Platforms

This command applies to the NetVanta 1000R, 3000, 4000, and 5000 Series units.

Command History

Release 1.1	Command was introduced.
Release 5.1	Command was expanded to include the PPP interface.

Usage Examples

The following example deactivates the configured dial-backup interface:

```
(config)#interface ppp 1
(config-ppp 1)#dial-backup shutdown
```

dynamic-dns [dyndns | dyndns-custom | dyndns-static] *<hostname> <username> <password>*

Use the **dynamic-dns** command to configure Dynamic DNS service provided by Dynamic Network Services, Inc. (www.dyndns.org).

Syntax Description

Refer to Functional Notes below for argument descriptions.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

dyndns - The Dynamic DNS^{SM} service allows you to alias a dynamic IP address to a static hostname in various domains. This allows your unit to be more easily accessed from various locations on the Internet. This service is provided for up to five hostnames.

dyndns-custom - DynDNS.org's Custom DNS^{SM} service provides a full DNS solution, giving you complete control over an entire domain name. A web-based interface provides two levels of control over your domain, catering to average or advanced users. Five globally redundant DNS servers ensure that your domain will always resolve.

A choice of two interfaces is available. The basic interface is designed for most users. It comes preconfigured for the most common configuration and allows for easy creation of most common record types. The advanced interface is designed for system administrators with a solid DNS background, and provides layout and functionality similar to a BIND zone file allowing for the creation of nearly any record type.

Custom DNS^{SM} can be used with both static and dynamic IPs and has the same automatic update capability through Custom DNS-aware clients as Dynamic DNS.

dyndns-static - The Static DNS service is similar to Dynamic DNS service in that it allows a hostname such as yourname.dyndns.org to point to your IP address. Unlike a Dynamic DNS host, a Static DNS host does not expire after 35 days without updates, but updates take longer to propagate though the DNS system. This service is provided for up to five hostnames.

If your IP address does not change often or at all but you still want an easy name to remember it by (without having to purchase your own domain name) Static DNS service is ideal for you.

If you would like to use your own domain name (such as yourname.com), you need Custom DNS service, which also provides full dynamic and static IP address support.

Usage Examples

The following example sets the dynamic-dns to **dyndns-custom** with hostname **host**, username **user**, and password **pass**:

```
(config)#interface tunnel 1
(config-tunnel 1)#dynamic-dns dyndns-custom host user pass
```

ip access-group *<listname>* [in | out]

Use the **ip access-group** command to create an access list to be used for packets transmitted on or received from the specified interface. Use the **no** form of this command to disable this type of control.

Syntax Description

<listname>	Assigns an IP access list name.
in	Enables access control on packets received on the specified interface.
out	Enables access control on packets transmitted on the specified interface.

Default Values

By default, these commands are disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

When this command is enabled, the IP destination address of each packet must be validated before being passed through. If the packet is not acceptable per these settings, it is dropped.

Usage Examples

The following example sets up the unit to only allow Telnet traffic (as defined in the user-configured **TelnetOnly** IP access list) into the tunnel interface:

```
(config)#ip access-list extended TelnetOnly
(config-ext-nacl)#permit tcp any any eq telnet
(config-ext-nacl)#interface tunnel 1
(config-tunnel 1)#ip access-group TelnetOnly in
```

ip address *<address> <mask>* secondary

Use the **ip address** command to define an IP address on the specified interface. Use the **no** form of this command to remove a configured IP address.

Syntax Description

<address>	Defines the IP address for the interface in dotted decimal notation (for example: 192.22.73.101).
<mask>	Specifies the subnet mask that corresponds to the listed IP address.
secondary	Optional. Configures a secondary IP address for the specified interface.

Default Values

By default, there are no assigned IP addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Usage Examples

The following example configures an IP address of **192.22.72.101/30**:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip address 192.22.72.101 255.255.255.252
```

ip helper-address *<address>*

Use the **ip helper-address** command to configure the AOS to forward User Datagram Protocol (UDP) broadcast packets received on the interface. Use the **no** form of this command to disable forwarding packets.

> NOTE *The **ip helper-address** command must be used in conjunction with the **ip forward-protocol** command to configure the AOS to forward UDP broadcast packets. Refer to ip forward-protocol udp <port number>* on page 378 *for more information.*

Syntax Description

<address>	Specifies the destination IP address (in dotted decimal notation) for the forwarded UDP packets.

Default Values

By default, broadcast UDP packets are not forwarded.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

When used in conjunction with the **ip forward-protocol** command, the **ip helper-address** feature allows you to customize which broadcast packets are forwarded.

To implement the helper address feature, assign helper address(es) (specifying the device that needs to receive the broadcast traffic) to the interface closest to the host that transmits the broadcast packets. When broadcast packets (of the specified type forwarded using the **ip forward-protocol** command) are received on the interface, they will be forwarded to the device that needs the information.

Only packets meeting the following criteria are considered eligible by the **ip helper-address** feature:

1. The packet IP protocol is User Datagram Protocol (UDP).
2. Any UDP port specified using the **ip forward-protocol** command.
3. The media access control (MAC) address of the frame is an all-ones broadcast address (ffff.ffff.ffff).
4. The destination IP address is broadcast defined by all ones (255.255.255.255) or a subnet broadcast (for example, 192.33.4.251 for the 192.33.4.248/30 subnet).

Usage Examples

The following example forwards all DNS broadcast traffic to the DNS server with IP address 192.33.5.99:

```
(config)#ip forward-protocol udp domain
(config)#interface tunnel 1
(config-tunnel 1)#ip helper-address 192.33.5.99
```

ip igmp

Use the **ip igmp** command to configure multicasting-related functions for the interface.

Syntax Description

immediate-leave	Specifies that if only one host (or IGMP snooping switch) is connected to the interface, when a leave is received, multicast of that group is immediately terminated as opposed to sending a group query and timing out the group if no device responds. Works in conjunction with **ip igmp last-member-query-interval**. Applies to all groups when configured.
last-member-query-interval <*milliseconds*>	Controls the timeout used to detect whether any group receivers remain on an interface after a receiver leaves a group. If a receiver sends a leave-group message (IGMP Version 2), the router sends a group-specific query on that interface. After twice the time specified by this command plus as much as one second longer, if no receiver responds, the router removes that interface from the group and stops sending that group's multicast packets to the interface. Range: 100 to 65,535 ms. Default: 1000 ms.
querier-timeout <*seconds*>	Specifies the number of seconds that the router waits after the current querier's last query before it takes over as querier (IGMP V2). Range: 60 to 300 seconds. Default: 2x the **query-interval** value.
query-interval <*seconds* >	Specifies the interval at which IGMP queries are sent on an interface. Host query messages are addressed to the all-hosts multicast group with an IP TTL of 1. The router uses queries to detect whether multicast group members are on the interface and to select an IGMP designated router for the attached segment (if more than one multicast router exists). Only the designated router for the segment sends queries. For IGMP V2, the designated router is the router with the lowest IP address on the segment. Range: 0 to 65,535 seconds. Default: 60 seconds.
query-max-response-time <*seconds*>	Specifies the maximum response time advertised by this interface in queries when using IGMP V2. Hosts are allowed a random time within this period to respond, reducing response bursts. Default: 10 seconds.
static-group <*group-address*>	Configures the router's interface to be a statically-connected member of the specified group. Packets received on the correct RPF interface are forwarded to this interface regardless of whether any receivers have joined the specified group using IGMP.
version [1 | 2]	Sets the interface's IGMP version. The default setting is version 2.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 8.1	ATM sub-interface was added.
Release 9.1	Tunnel sub-interface was added.

Usage Examples

The following example sets the query message interval on the interface to 200 milliseconds:

```
config)#interface tunnel 1
(config-tunnel 1)#ip igmp last-member-query-interval 200
```

ip mcast-stub downstream

Use the **ip mcast-stub downstream** command to enable multicast forwarding and IGMP (router mode) on an interface, and to place it in multicast stub downstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub upstream** commands. Downstream interfaces connect to segments with multicast hosts. Multiple interfaces may be configured in downstream mode; however, interfaces connecting to the multicast network (upstream) should not be configured in downstream mode. Interfaces configured as downstream should have the lowest IP address of all IGMP-capable routers on the connected segment in order to be selected as the designated router and ensure proper forwarding.

Usage Examples

The following example enables multicast forwarding and IGMP on the interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip mcast-stub downstream
```

ip mcast-stub helper-enable

Use the **ip mcast-stub helper-enable** command to assign the **ip mcast-stub helper-address** as the IGMP proxy. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address, ip mcast-stub upstream**, and **ip mcast-stub downstream** commands. When enabled, the interface becomes a helper forwarding interface. The IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the unit to perform as an IGMP proxy.

Usage Examples

The following example sets the helper address as the IGMP proxy:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip mcast-stub helper-enable
```

ip mcast-stub upstream

Use the **ip mcast-stub upstream** command to enable multicast forwarding on an interface and place it in multicast stub upstream mode. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

This command is used in IP multicast stub applications in conjunction with the **ip mcast-stub helper-address** and **ip mcast-stub downstream** commands. When enabled, the interface becomes a candidate to be a helper forwarding interface. If chosen as the best path toward the helper address by the router's unicast route table, the IGMP host function is dynamically enabled and the interface becomes the active upstream interface, enabling the router to perform as an IGMP proxy. Though multiple interfaces may be candidates, no more than one interface will actively serve as the helper forwarding interface.

Usage Examples

The following example enables multicast forwarding on the interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip mcast-stub upstream
```

ip ospf

Use the **ip ospf** command to customize OSPF settings (if needed).

Syntax Description

authentication-key	Specifies a simple-text authentication password to be used by other routers using <*password*> the OSPF simple password authentication.
cost <*value*>	Specifies the OSPF cost of sending a packet on the interface. This value overrides any computed cost value. Range: 1 to 65,535.
dead-interval <*seconds*>	Sets the maximum interval allowed between hello packets. If the maximum is exceeded, neighboring devices will determine that the device is down. Range: 0 to 32,767.
hello-interval <*seconds*>	Specifies the interval between hello packets sent on the interface. Range: 0 to 32,767.
message-digest-key <*keyid*> **md5** <*key*>	Configures OSPF Message Digest 5 (MD5) authentication (16-byte max) keys.
priority <*value*>	Set the OSPF priority. The value set in this field helps determine the designated router for this network. Range: 0 to 255.
retransmit-interval <*seconds*>	Specifies the time between link-state advertisements (LSAs). Range: 0 to 32,767.
transmit-delay <*seconds*>	Sets the estimated time required to send an LSA on the interface. Range: 0 to 32,767.

Default Values

retransmit-interval <*seconds*>	5 seconds
transmit-delay <*seconds*>	1 second
hello-interval <*seconds*>	10 seconds: Ethernet, point-to-point, Frame Relay, Tunnel, and PPP
dead-interval <*seconds*>	40 seconds

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Usage Example

The following example sets the maximum number of seconds allowed between hello packets to 25,000:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip ospf dead-interval 25000
```

ip ospf authentication [message-digest | null]

Use the **ip ospf authentication** command to authenticate an interface that is performing OSPF authentication.

Syntax Description

message-digest	Optional. Selects message-digest authentication type.
null	Optional. Specifies that no authentication is used.

Default Values

By default, this is set to null (meaning no authentication is used).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Usage Examples

The following example specifies that no authentication will be used on the tunnel interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip ospf authentication null
```

ip ospf network [broadcast | point-to-point]

Use the **ip ospf network** command to specify the type of network on this interface.

Syntax Description

broadcast	Sets the network type for broadcast.
point-to-point	Sets the network type for point-to-point.

Default Values

By default, Ethernet defaults to broadcast. PPP, Frame Relay, and tunnel default to point-to-point.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 3.1	Command was introduced.
Release 9.1	Command was expanded to include tunnel interfaces.

Functional Notes

A point-to-point network will not elect designated routers.

Usage Examples

The following example designates a broadcast network type:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip ospf network broadcast
```

ip pim sparse-mode

Use the **ip pim sparse-mode** command to enable protocol-independent multicast (PIM) sparse mode for this interface. Use the **no** form of this command to disable PIM sparse mode.

Syntax Description

No subcommands.

Default Values

By default, PIM sparse mode for this interface is disabled.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

PIM Sparse Mode is a multicast routing protocol that makes use of the unicast forwarding table. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) for a multicast group or a shortest-path tree rooted at a specific source for a multicast group.

Usage Examples

The following example enables PIM sparse mode on the interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip pim sparse-mode
```

ip pim-sparse dr-priority *<priority number>*

Use the **ip pim-sparse dr-priority** command to specify the priority for the designated router (DR). This command modifies the routers priority in the DR election process. Use the **no** form of this command to return to the default value.

Syntax Description

<priority number>	Specifies the priority number for the DR router. Valid range is 1 to 4,294,967,295.

Default Values

By default, the DR priority is set to 1.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the DR priority to 5:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip pim-sparse dr-priority 5
```

ip pim-sparse hello-timer *<time>*

Use the **ip pim-sparse hello-timer** command to specify protocol-independent multicast (PIM) sparse hello timer period. This is the time interval at which periodic hellos are sent out on all interfaces of a PIM-capable router. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the time in seconds between hello transmissions. Valid range is 10 to 12,600 seconds.

Default Values

By default, the hello timer is set to 30 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the hello timer to 60 seconds:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip pim-sparse hello-timer 60
```

ip pim-sparse nbr-timeout *<time>*

Use the **ip pim-sparse nbr-timeout** command to specify protocol-independent multicast (PIM) sparse neighbor timeout. This is the time interval after which a PIM-capable router will consider a neighbor not present. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the time interval in seconds after which a neighbor is considered not present. Valid range is 30 to 10,800 seconds.

Default Values

By default, the nbr-timeout is set to 105 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the nbr-timeout to 300 seconds:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip pim-sparse nbr-timeout 300
```

ip pim-sparse override-interval *<time>*

Use the **ip pim-sparse override-interval** command to specify the protocol-independent multicast (PIM) sparse join/prune override interval. This delay interval is the period after a join/prune that another router on the LAN may override a join/prune. Use the **no** form of this command to return to the default value.

Syntax Description

<time>	Specifies the delay time in milliseconds. Valid range is 0 to 65,535 milliseconds.

Default Values

By default, the override-interval is set to 2500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the override-interval to 3000 milliseconds:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip pim-sparse override-interval 3000
```

ip pim-sparse propagation-delay <*time*>

Use the **ip pim-sparse propagation-delay** command to specify protocol-independent multicast (PIM) sparse join/prune propagation delay. This is the expected propagation delay in milliseconds over the local link. Use the **no** form of this command to return to the default value.

Syntax Description

<*time*>	Specifies the expected propagation delay in milliseconds. Valid range is 0 to 32,767 milliseconds.

Default Values

By default, the propagation-delay is set to 500 milliseconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the propagation-delay to 1000 milliseconds:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip pim-sparse propagation-delay 1000
```

ip policy route-map *<policy name>*

Use the **ip policy route-map** command to assign a policy route-map to this interface. Use the **no** form of this command to remove the route-map policy.

Syntax Description

<policy name>	Specifies the name of the policy route map to assign to this interface.

Default Values

By default, no policy route map is assigned to this interface.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example assigns the policy route map **policy1** to the interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip policy route-map policy1
```

ip proxy-arp *<ip address> <subnet mask>*

Use the **ip proxy-arp** command to enable proxy Address Resolution Protocol (ARP) on the interface. Use the **no** form of this command to disable this feature.

Syntax Description

<ip address>	Defines the proxy ARP IP address in dotted decimal notation (for example: 192.22.73.101).
<subnet mask>	Specifies the subnet mask that corresponds to the listed IP address.

Default Values

By default, proxy-arp is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

In general, the principle of proxy ARP allows a router to insert its IP address in the source IP address field of a packet (if the packet is from a host on one of its subnetworks). This allows hosts to reach devices on other subnetworks without implementing routing or specifying a default gateway.

If proxy ARP is enabled, the AOS will respond to all proxy ARP requests with its specified MAC address and forward packets accordingly.

Enabling proxy ARP on an interface may introduce unnecessary ARP traffic on the network.

Usage Examples

The following enables proxy ARP on the tunnel interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip proxy-arp
```

ip rip receive version [1 | 2]

Use the **ip rip receive version** command to configure the RIP version the unit accepts in all RIP packets received on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Only accept received RIP version 1 packets on the interface.
2	Only accept received RIP version 2 packets on the interface.

Default Values

By default, all interfaces implement RIP version 1 (the default value for the version command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip receive version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. See *version [1 | 2]* on page 1144 for more information.

The AOS only accepts one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the tunnel interface to accept only RIP version 2 packets:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip rip receive version 2
```

ip rip send version [1 | 2]

Use the **ip rip send version** command to configure the RIP version the unit sends in all RIP packets transmitted on the interface. Use the **no** form of this command to restore the default value.

Syntax Description

1	Only transmits RIP version 1 packets on the interface.
2	Only transmits RIP version 2 packets on the interface.

Default Values

By default, all interfaces transmit RIP version 1 (the default value for the **version** command).

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Use the **ip rip send version** command to specify a RIP version that overrides the **version** (in the Router RIP) configuration. See *version [1 | 2]* on page 1144 for more information.

The AOS only transmits one version (either 1 or 2) on a given interface.

Usage Examples

The following example configures the tunnel interface to transmit only RIP version 2 packets:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip rip send version 2
```

ip route-cache

Use the **ip route-cache** command to enable fast-cache switching on the interface. Use the **no** form of this command to disable fast-cache switching and return to process switching mode.

> *Using Network Address Translation (NAT) or the AOS firewall capabilities on an interface requires process switching mode (using the* ***no ip route-cache*** *command).*

Syntax Description

No subcommands.

Default Values

By default, fast-cache switching is enabled on all Ethernet and virtual Frame Relay sub-interfaces. IP route-cache is enabled for all virtual PPP interfaces.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Fast switching allows an IP interface to provide optimum performance when processing IP traffic.

Usage Examples

The following example enables fast switching on the tunnel interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#ip route-cache
```

keepalive *<period> <retries>*

Use the **keepalive** command to periodically send keepalive packets to verify the integrity of the tunnel from end to end. Use the **no** form of this command to disable keepalives.

Syntax Description

<period>	Defines the time interval (in seconds) between transmitted keepalive packets (valid range: 1 to 32,767 seconds).
<retries>	Defines the number of times to retry after failed keepalives before determining that the tunnel endpoint is down (valid range: 1 to 255 times).

Default Values

By default, keepalives are disabled. When enabled, the keepalive period defaults to 10 seconds and the retry count defaults to 3 times.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Keepalives do not have to be configured on both ends of the tunnel in order to work. A tunnel is not aware of incoming keepalive packets.

Usage Examples

The following example enables **keepalive** with a period of 30 seconds and a retry count of 5 times:

```
(config)#interface tunnel 1
(config-tunnel 1)#keepalive 30 5
```

lldp receive

Use the **lldp receive** command to allow LLDP packets to be received on this interface.

Syntax Description

No subcommands.

Default Values

By default, all interfaces are configured to send and receive LLDP packets.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example configures the tunnel interface to receive LLDP packets:

```
(config)#interface tunnel 1
(config-tunnel 1)#lldp receive
```

lldp send [management-address I port-description I system-capabilities I system-description I system-name I and-receive]

Use the **lldp send** command to configure this interface to transmit LLDP packets or to control the types of information contained in the LLDP packets transmitted by this interface.

Syntax Description

management-address	Enables transmission of management address information on this interface.
port-description	Enables transmission of port description information on this interface.
system-capabilities	Enables transmission of this device’s system capabilities on this interface.
system-description	Enables transmission of this device’s system description on this interface.
system-name	Enables transmission of this device’s system name on this interface.
and-receive	Configures this interface to both transmit and receive LLDP packets.

Default Values

Be default, all interfaces are configured to transmit and receive LLDP packets of all types.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Individual LLDP information can be enabled or disabled using the various forms of the **lldp send** command. For example, use the **lldp send and-receive** command to enable transmit and receive of all LLDP information. Then use the **no lldp send port-description** command to prevent LLDP from transmitting port description information.

Usage Examples

The following example configures the tunnel interface to transmit LLDP packets containing all enabled information types:

```
(config)#interface tunnel 1
(config-tunnel 1)#lldp send
```

The following example configures the tunnel interface to transmit and receive LLDP packets containing all information types:

```
(config)#interface tunnel 1
(config-tunnel 1)#lldp send and-receive
```

mtu *<size>*

Use the **mtu** command to configure the maximum transmit unit (MTU) size for the active interface. Use the **no** form of this command to return to the default value.

Syntax Description

<size> Configures the window size for transmitted packets. The valid ranges for the various interfaces are listed below:

ATM interfaces	64 to 1520
Demand interfaces	64 to 1520
Ethernet interfaces	64 to 1500
FDL interfaces	64 to 256
HDLC interfaces	64 to 1520
Loopback interfaces	64 to 1500
Tunnel interfaces	64 to 18,190
Virtual Frame Relay sub-interfaces	64 to 1520
Virtual PPP interfaces	64 to 1500

Default Values

<size> The default values for the various interfaces are listed below:

ATM interfaces	1500
Demand interfaces	1500
Ethernet interfaces	1500
FDL interfaces	256
HDLC interfaces	1500
Loopback interfaces	1500
Tunnel interfaces	1500
Virtual Frame Relay sub-interfaces	1500
Virtual PPP interfaces	1500

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1 Command was introduced.

Functional Notes

OSPF will not become adjacent on links where the MTU sizes do not match. If router A and router B are exchanging hello packets but their MTU sizes do not match, they will never reach adjacency. This is by design and required by the RFC.

Usage Examples

The following example specifies an MTU of 1200 on the tunnel interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#mtu 1200
```

tunnel checksum

Use the **tunnel checksum** command to verify the checksum of incoming Generic Routing Encapsulation (GRE) packets and to include a checksum on outgoing packets. Use the **no** form of this command to disable checksum.

Syntax Description

No subcommands.

Default Values

By default, **tunnel checksum** is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Both ends of the tunnel must have **tunnel checksum** enabled in order for a meaningful configuration. When both endpoints have **tunnel checksum** enabled, a packet with an incorrect checksum will be dropped. If the endpoints differ in their checksum configuration, all packets will still flow without any checksum verification.

Usage Examples

The following example enables checksum on the tunnel 1 interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel checksum
```

Technology Review

When enabled, the **tunnel checksum** will be calculated for each outgoing GRE packet with the result stored in the GRE header. The checksum present bit will also be set in the header.

tunnel destination *<ip address>*

Use the **tunnel destination** command to specify the IP address to use as the destination address for all packets transmitted on this interface. Use the **no** form of this command to clear the **tunnel destination** address.

Syntax Description

<ip address>	Specifies the IP address in dotted decimal notation to use as the destination address for all packets transmitted on this interface (for example: 192.22.73.101).

Default Values

By default, no tunnel destinations are defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Until a tunnel interface has a destination IP address defined, it is not operational.

The tunnel destination IP address will be the value put into the destination field of the outer IP header after GRE encapsulation of the original packet. A route must be defined for the destination address. Be certain there are no recursive routes by ensuring that a tunnel’s destination address will be routed out a physical interface. There is a possibility of creating a routing loop when tunnel interface traffic gets routed back to the same tunnel interface or to another tunnel interface, which in turn, does not have a route out a physical interface. In either case, the tunnel will go down for a period of one minute, after which it will come back up to determine if the recursive routes have been resolved. This allows time for routing protocols to converge on a valid route. If a static route has caused the recursive routing loop, the tunnel status may oscillate until the route is changed.

Usage Examples

The following example sets the tunnel destination IP address to **192.22.73.101**:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel destination 192.22.73.101
```

tunnel key *<value>*

Use the **tunnel key** command to specify a value shared by both endpoints of the tunnel that will provide minimal security and delineate between tunnels with the same source and destination addresses. Use the **no** form of this command to disable the key.

Syntax Description

<value>	Defines the key value for this tunnel (valid range: 1 to 4,294,967,294).

Default Values

By default, a key is not configured.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

A matching key value must be defined on both endpoints of the tunnel or packets will be discarded.

Usage Examples

The following example sets the key on a tunnel interface to a value of 1234:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel key 1234
```

Technology Review

When enabled, the key will be stored in the GRE header and the key present bit will be set.

tunnel mode gre

Use the **tunnel mode gre** command to encapsulate traffic destined for the tunnel interface in a Generic Routing Encapsulation (GRE) header. Use the **no** form of this command to set the tunnel to its default mode.

Syntax Description

No subcommands.

Default Values

By default, the tunnel interface will be configured for GRE mode.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

GRE is currently the only allowed mode for tunnel interface operation.

Usage Examples

The following example configures the tunnel interface for GRE mode:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel mode gre
```

tunnel sequence-datagrams

Use the **tunnel sequence-datagrams** command to enable sequence number checking on incoming Generic Routing Encapsulation (GRE) packets, to drop packets arriving out of order, and to include a sequence number in outgoing packets. Use the **no** form of this command to disable sequence number checking.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Functional Notes

Both ends of the tunnel must have sequence numbering enabled. When both endpoints have sequence numbering enabled, a packet arriving with a sequence number less than the current expected value will be dropped. If the endpoints differ in their sequence numbering configuration, all packets will still flow without any sequence number verification. Be careful enabling sequence number verification on a tunnel. The tunnel can easily become out of sequence due to network conditions outside of the tunnel endpoints. It may be difficult to establish a successful traffic flow after an out of sequence condition occurs.

Technology Review

When enabled, the next valid sequence number will be placed in the GRE header of each outgoing packet, and the sequence number present bit will be set.

Usage Examples

The following example enables sequence number processing on the tunnel interface:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel sequence-datagrams
```

tunnel source [*<ip address>* | *<interface>*]

Use the **tunnel source** command to specify the IP address or name of a physical interface to use as the source address for all packets transmitted on this interface. Use the **no** form of this command to clear the tunnel source address.

Syntax Description

<ip address>	Specifies the IP address in dotted decimal notation to use as the source address for all packets transmitted on this interface (for example: 192.22.73.101).
<interface>	Specifies the interface (in the format type *<slot/port>*) that contains the IP address to use as the source address for all packets transmitted on this interface.

Default Values

By default, a tunnel source is not defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.
Release 11.1	Command was expanded to include demand interfaces.

Functional Notes

Until a tunnel interface has a source IP address defined and the physical interface used as the source is operational, the tunnel is not operational.

The tunnel source IP address will be the value put into the source field of the outer IP header after GRE encapsulation of the original packet.

Usage Examples

The following example sets the tunnel source IP address to **192.22.73.101**:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel source 192.22.73.101
```

The following example sets the tunnel source IP address to the address of the Ethernet interface labeled 0/1:

```
(config)#interface tunnel 1
(config-tunnel 1)#tunnel source eth 0/1
```

CA Profile Configuration Command Set

To activate the Certificate Authority (CA) Profile Configuration mode, enter the **crypto ca profile** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ca profile MyProfile
Configuring New CA Profile MyProfile
(ca-profile)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

crl optional on page 1029

email address <email address> on page 1030

enrollment retry [count | period] on page 1031

enrollment terminal on page 1032

enrollment url <url> on page 1033

fqdn <fqdn> on page 1034

ip-address <address> on page 1035

password <password> on page 1036

serial-number on page 1037

subject-name <name> on page 1038

crl optional

Use the **crl optional** command to make CRL verification optional.

Syntax Description

No subcommands.

Default Values

By default, CRL optional is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

If enabled, the AOS is able to accept certificates even if no CRL is loaded into the configuration. Currently, this is the only mode supported by the AOS for CRL negotiations.

Usage Examples

The following example sets CRL verification as optional:

```
(ca-profile)#crl optional
```

email address *<email address>*

Use the **email address** command to specify that an email address should be included in the certificate request.

Syntax Description

<email address>	Specifies the complete email address to use when sending certificate requests. This field allows up to 51 characters.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the email address only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <name>* on page 316.

Usage Examples

The following example specifies **joesmith@company.com** as the email address to be sent in certificate requests:

```
(ca-profile)#email address joesmith@company.com
```

enrollment retry [count | period]

Use the **enrollment retry** command to determine how the AOS handles certificate requests.

Syntax Description

count <*count*>	Specifies the number of times the AOS re-sends a certificate request when it does not receive a response from the previous request. Range: 1 to 100.
period <*minutes*>	Specifies the time period between certificate request retries. The default is 1 minute between retries. Range: 1 to 60 minutes.

Default Values

By default, period is set to 5 minutes, and count is set to 12 retries.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example configures the AOS to send certificate requests every two minutes, stopping after 50 retries (if no response is received):

```
(ca-profile)#enrollment retry count 50
(ca-profile)#enrollment retry period 2
```

enrollment terminal

Use the **enrollment terminal** command to specify manual (i.e., cut-and-paste) certificate enrollment.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

This mode is overridden if the **enrollment url** command specifies the CA to which automatic certificate requests are to be sent via simple certificate exchange protocol (SCEP). Issuing an **enrollment terminal** command after using the **enrollment url** command deletes the URL and forces the unit to use manual enrollment. Refer to *enrollment url <url>* on page 1033 for more information.

Usage Examples

The following example configures the AOS to accept manual certificate enrollment input:

```
(ca-profile)#enrollment terminal
```

enrollment url *<url>*

Use the **enrollment url** command to specify the URL of the CA to which the AOS should send certificate requests.

Syntax Description

<url>	Specifies the certificate authority's URL (e.g., http://10.10.10.1:400/abcdefg/pkiclient.exe).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

When entering the URL **http://** is required, followed by the IP address or DNS name of the CA. If the port number is something other than 80, include it after the IP address or DNS name separated with a colon (**:**).

The CA may have other necessary information to include in the CGI path before ending with the actual CGI program. An example template to follow is **http://hostname:port/path/to/program.exe**.

Use the default program **pkiclient.exe** without specifying it, end the URL with a slash (**/**). Otherwise, you must enter the program name to use. For example, **http://10.10.10.1:400/abcdefg/** will assume **pkiclient.exe** as the program (but not including the terminating slash is a configuration error).

Specifying this command will override the **enrollment terminal** setting as described previously (refer to *enrollment terminal* on page 1032).

Usage Examples

The following example specifies **http://CAserver/certsrv/mscep/mscep.dll** as the URL to which the AOS will send certificate requests:

```
(ca-profile)#enrollment url http://CAserver/certsrv/mscep/mscep.dll
```

fqdn *<fqdn>*

Use the **fqdn** command to specify a fully-qualified domain name (FQDN) to be included in the certificate requests.

Syntax Description

<fqdn>	Specifies the FQDN (e.g., company.com) to be included in requests.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the FQDN only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <name>* on page 316.

Usage Examples

The following example specifies **company.com** as the FQDN to be sent in certificate requests:

```
(ca-profile)#fqdn company.com
```

ip-address *<address>*

Use the **ip-address** command to specify an IP address to be included in the certificate requests.

Syntax Description

<address>	Defines the IP address in dotted decimal notation (e.g., 192.22.73.101).

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the IP address only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <name>* on page 316.

Usage Examples

The following example specifies **66.203.52.193** as the IP address to be sent in certificate requests:

```
(ca-profile)#ip-address 66.203.52.193
```

password *<password>*

Use the **password** command to specify the challenge password for simple certificate exchange protocol (SCEP). Use the **no** form of this command to allow CA requests to be sent automatically (using SCEP) without requiring a password.

Syntax Description

<password>	Specifies the SCEP password (up to 80 characters).

Default Values

By default, no password is required.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

There are two places for configuring a SCEP password:

- At the **(ca-profile)#** prompt.
- If it is not configured at the **(ca-profile)#** prompt, you are prompted to enter one when going through the certificate enrollment process.

The password is sent to the CA from which you are requesting a certificate. The CA may then ask for the password later before a certificate can be revoked. Refer to *crypto ca enroll <name>* on page 316.

Usage Examples

The following example sets the SCEP challenge password to **adtran**:

```
(ca-profile)#password adtran
```

serial-number

Use the **serial-number** command to specify that a serial number will be included in the certificate request.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

By default, this command is set to **no serial-number**, which means that the serial number is not included in the certificate requests.

Usage Examples

The following example configures AOS to include a serial number in the certificate request:

```
(ca-profile)#serial-number
```

subject-name *<name>*

Use the **subject-name** command to specify the subject name used in the certificate request.

Syntax Description

<name>	Specifies a subject name string using up to 256 characters entered in X.500 LDAP format.

Default Values

By default, there is no subject name configured.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

Configuring this setting simplifies the **crypto ca enroll** dialog, allowing you to enter the subject name only once rather than every time you go through the enrollment process. Refer to *crypto ca enroll <name>* on page 316.

Usage Examples

The following example assigns a subject name of **Adtran-cert** to certificate requests:

```
(ca-profile)#subject-name Adtran-cert
```

CERTIFICATE CONFIGURATION COMMAND SET

To activate the Certificate Configuration mode, enter the **crypto ca certificate chain** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ca certificate chain MyProfile
(config-cert-chain)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

certificate <serial-number> on page 1040

certificate ca <serial-number> on page 1041

crl on page 1042

certificate *<serial-number>*

Use the **certificate** command to restore a certificate. Use the **no** form of this command to remove a specific certificate from the certificate chain.

Syntax Description

<serial-number>	Specifies the certificate's serial number (up to 51 characters). This value can be found for existing certificates by using the **show run** command.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The user typically does not enter this command. It is primarily used to restore certificates from the startup configuration when the product is powered up.

Usage Examples

The following example removes the certificate with the serial number **73f0bfe5ed8391a54d1214390a36cee7**:

```
(config)#crypto ca certificate chain MyProfile
(config-cert-chain)#no certificate 73f0bfe5ed8391a54d1214390a36cee7
```

certificate ca *<serial-number>*

Use the **certificate ca** command to restore a CA certificate. Use the **no** form of this command to remove a specific certificate from the certificate chain for a CA.

Syntax Description

<serial-number>	Specifies the certificate's serial number (up to 51 characters). This value can be found for existing certificates by using the **show run** command.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The user typically does not enter this command. It is primarily used to restore certificates from the startup configuration when the product is powered up.

Usage Examples

The following example removes the CA certificate with the serial number **0712**:

```
(config)#crypto ca certificate chain MyProfile
(config-cert-chain)#no certificate ca 0712
```

crl

Use the **crl** command to restore a CRL. Use the **no** form of this command to remove the CRL for the specific CA.

Syntax Description

No subcommands.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The user typically does not enter this command. It is primarily used to restore CRLs from the startup configuration when the product is powered up.

Usage Examples

The following example removes the CRL for the current CA:

```
(config)#crypto ca certificate chain MyProfile
(config-cert-chain)#no crl
```

CRYPTO MAP IKE COMMAND SET

To activate the Crypto Map IKE mode, enter a valid version of the **crypto map ipsec-ike** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto map Map-Name 10 ipsec-ike
(config-crypto-map)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

antireplay on page 1044

ike-policy <policy number> on page 1045

match address <listname> on page 1046

set peer <address> on page 1048

set pfs [group1 | group2] on page 1049

set security-association lifetime [kilobytes | seconds] <value> on page 1050

set transform-set <setname1 - setname6> on page 1051

> NOTE
>
> *For VPN configuration example scripts, refer to the technical support note **Configuring VPN** located on the **ADTRAN OS Documentation** CD provided with your unit.*

antireplay

Use the **antireplay** command to enable antireplay sequence number checking for all security associations created on this crypto map. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series and units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables antireplay sequence checking on crypto map VPN 100:

```
(config)#crypto map VPN 100 ipsec-ike
(config-crypto-map)#antireplay
```

ike-policy *<policy number>*

Use the **ike-policy** command to ensure that only a specified IKE policy is used to establish the IPSec tunnel. This prevents any mobile VPN policies from using IPSec policies that are configured for static VPN peer policies.

Syntax Description

<policy number>	Specifies the policy number of the policy to assign to this crypto map.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example shows a typical crypto map configuration:

```
(config)#crypto ike policy 100
(config)#crypto map VPN 10 ipsec-ike
(config-crypto-map)#description “Remote Office”
(config-crypto-map)#match address VPN-10-vpn-selectors
(config-crypto-map)#set peer 10.22.17.13
(config-crypto-map)#set transform-set esp-3des-esp-md5-hmac
(config-crypto-map)#ike-policy 100
```

match address *<listname>*

Use the **match address** command to assign an IP access list to a crypto map definition. The access list designates the IP packets to be encrypted by this crypto map. Refer to *ip access-list extended <listname>* on page 344 for more information on creating access lists.

Syntax Description

<listname>	Specifies the name of the access list you wish to assign to this crypto map.

Default Values

By default, no IP access lists are defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list (ACL) is assigned to the crypto map using the **match address** command. If no ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the ADTRAN product. The source information must be the local ADTRAN product and the destination must be the peer.

Only extended access lists can be used in crypto maps.

Usage Examples

The following example shows setting up an ACL (called **NewList**) and then assigning the new list to a crypto map (called **NewMap**):

```
(config)#ip access-list extended NewList

Configuring New Extended ACL "NewList"
(config-ext-nacl)#exit
(config)#crypto map NewMap 10 ipsec-ike
(config-crypto-map)#match address NewList
```

Technology Review

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: **ipsec-manual** and **ipsec-ike**. Each entry is given an index, which is used to sort the ordered list.

When a nonsecured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the nonsecured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable SA exists, that 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 an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

set peer *<address>*

Use the **set peer** command to set the IP address of the peer device. This must be set for multiple remote peers.

Syntax Description

<address>	Specifies the IP address of the peer device. If this is not configured, it implies responder only to any peer.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

If no peer IP addresses are configured, the entry will only be used to respond to IPSec requests; it cannot initiate the requests (since it doesn't know which IP address to send the packet to). If a single peer IP address is configured, the crypto map entry can be used to both initiate and respond to SAs.

The peer IP address is the public IP address of the device which will terminate the IPSec tunnel. If the peer IP address is not static, the ADTRAN product cannot initiate the VPN tunnel. By setting no peer IP address, the ADTRAN product can respond to an IPSec tunnel request.

Usage Examples

The following example sets the peer IP address of 10.100.23.64:

```
(config-crypto-map)#set peer 10.100.23.64
```

set pfs [group1 | group2]

Use the **set pfs** command to choose the type of perfect forward secrecy (if any) that will be required during IPSec negotiation of security associations for this crypto map. Use the **no** form of this command to require no PFS.

Syntax Description

group1	Requires IPSec to use Diffie-Hellman Group 1 (768-bit modulus) exchange during IPSec SA key generation.
group2	Requires IPSec to use Diffie-Hellman Group 2 (1024-bit modulus) exchange during IPSec SA key generation.

Default Values

By default, no PFS will be used during IPSec SA key generation.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

If left at the default setting, no perfect forward secrecy (PFS) will be used during IPSec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data linkage between prior keys and future keys.

Usage Examples

The following example specifies use of the Diffie-Hellman Group 1 exchange during IPSec SA key generation:

```
(config-crypto-map)#set pfs group 1
```

set security-association lifetime [kilobytes | seconds] *<value>*

Use the **set security-association lifetime** command to define the lifetime (in kilobytes and/or seconds) of the IPSec SAs created by this crypto map.

Syntax Description

kilobytes *<value>*	Specifies the SA lifetime limit in kilobytes.
seconds *<value>*	Specifies the SA lifetime limit in seconds.

Default Values

By default, the **security-association lifetime** is set to 28,800 seconds and there is no default for the kilobytes lifetime.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the security association.

Usage Examples

The following example sets the SA lifetime to 300 kilobytes and 2 hours:

```
(config-crypto-map)#set security-association lifetime kilobytes 300
(config-crypto-map)#set security-association lifetime seconds 7200
```

set transform-set *<setname1 - setname6>*

Use the **set transform-set** command to assign up to six transform sets to a crypto map. Refer to *crypto ipsec transform-set <setname> <parameters>* on page 329 for information on defining transform sets.

Syntax Description

<setname>	Assign up to six transform sets to this crypto map by listing the set names, separated by a space.

Default Values

By default, there is no transform set assigned to the crypto map.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms (see *crypto ipsec transform-set <setname> <parameters>* on page 329).

If no transform set is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

Usage Examples

The following example first creates a transform set (**Set1**) consisting of two security algorithms (up to three may be defined), and then assigns the transform set to a crypto map (**Map1**):

```
(config)#crypto ipsec transform-set Set1 esp-3des esp-sha-hmac
(cfg-crypto-trans)#exit
(config)#crypto map Map1 1 ipsec-ike
(config-crypto-map)#set transform-set Set1
```

CRYPTO MAP MANUAL COMMAND SET

To activate the Crypto Map Manual mode, enter a valid version of the **crypto map ipsec-manual** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto map Map-Name 10 ipsec-manual
(config-crypto-map)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

description <text> on page 31

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

antireplay on page 1053

ike-policy <policy number> on page 1054

match address <listname> on page 1055

set peer <address> on page 1057

set session-key [inbound | outbound] on page 1058

set transform-set <setname> on page 1062

> NOTE
>
> *For VPN configuration example scripts, refer to the technical support note* ***Configuring VPN*** *located on the* ***ADTRAN OS Documentation*** *CD provided with your unit.*

antireplay

Use the **antireplay** command to enable antireplay sequence number checking for all security associations created on this crypto map. Use the **no** form of this command to disable.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example enables antireplay sequence checking on crypto map VPN 100:

```
(config)#crypto map VPN 100 ipsec-manual
(config-crypto-map)#antireplay
```

ike-policy *<policy number>*

Use the **ike-policy** command to ensure that only a specified IKE policy is used to establish the IPSec tunnel. This prevents any mobile VPN policies from using IPSec policies that are configured for static VPN peer policies.

Syntax Description

<policy number>	Specifies the policy number of the policy to assign to this crypto map.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example shows a typical crypto map configuration:

```
(config)#crypto ike policy 100
(config)#crypto map VPN 10 ipsec-manual
(config-crypto-map)#description “Remote Office”
(config-crypto-map)#match address VPN-10-vpn-selectors
(config-crypto-map)#set peer 10.22.17.13
(config-crypto-map)#set transform-set esp-3des-esp-md5-hmac
(config-crypto-map)#ike-policy 100
```

match address *<listname>*

Use the **match address** command to assign an IP access list to a crypto map definition. The access list designates the IP packets to be encrypted by this crypto map. See *ip access-list extended <listname>* on page 344 for more information on creating access lists.

Syntax Description

<listname>	Specifies the name of the access list you wish to assign to this crypto map.

Default Values

By default, no IP access lists are defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the selectors used to determine which data to secure. Instead, the crypto map entry refers to an access control list. An access control list (ACL) is assigned to the crypto map using the **match address** command (see *crypto map* on page 331) with the NetVanta 2000 and 3000 Series units. If no ACL is configured for a crypto map, then the entry is incomplete and will have no effect on the system.

The entries of the ACL used in a crypto map should be created with respect to traffic sent by the ADTRAN product. The source information must be the local ADTRAN product, and the destination must be the peer.

Only extended access lists can be used in crypto maps.

Usage Examples

The following example shows setting up an access list (called **NewList**) and then assigning the new list to a crypto map (called **NewMap**):

```
(config)#ip access-list extended NewList

Configuring New Extended ACL "NewList"

(config-ext-nacl)#exit
(config)#crypto map NewMap 10 ipsec-manual
(config-crypto-map)#match address NewList
```

Technology Review

A crypto map entry is a single policy that describes how certain traffic is to be secured. There are two types of crypto map entries: **ipsec-manual** and **ipsec-ike**. Each entry is given an index, which is used to sort the ordered list.

When a nonsecured packet arrives on an interface, the crypto map set associated with that interface is processed in order. If a crypto map entry matches the nonsecured traffic, the traffic is discarded.

When a packet is to be transmitted on an interface, the crypto map set associated with that interface is processed in order. The first crypto map entry that matches the packet will be used to secure the packet. If a suitable SA exists, that 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 an SA. If an SA does not exist, or if the packet fails any of the security checks (bad authentication, traffic does not match SA selectors, etc.), it is discarded. If all checks pass, the packet is forwarded normally.

set peer *<address>*

Use the **set peer** command to set the IP address of the peer device.

Syntax Description

<address>	Specifies the IP address of the peer device.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

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.

Usage Examples

The following example sets the peer IP address of 10.100.23.64:

```
(config-crypto-map)#set peer 10.100.23.64
```

set session-key [inbound | outbound]

Use the **set session-key** command to define the encryption and authentication keys for this crypto map.

Variations of this command include the following:

set session-key inbound ah *<SPI> <keyvalue>*
set session-key inbound esp *<SPI>* **authenticator** *<keyvalue>*
set session-key inbound esp *<SPI>* **cipher** *<keyvalue>*
set session-key inbound esp *<SPI>* **cipher** *<keyvalue>* **authenticator** *<keyvalue>*
set session-key outbound ah *<SPI> <keyvalue>*
set session-key outbound esp *<SPI>* **authenticator** *<keyvalue>*
set session-key outbound esp *<SPI>* **cipher** *<keyvalue>*
set session-key outbound esp *<SPI>* **cipher** *<keyvalue>* **authenticator** *<keyvalue>*

Syntax Description

inbound	Defines encryption keys for inbound traffic.
outbound	Defines encryption keys for outbound traffic.
ah *<SPI>*	Specifies authentication header protocol.
esp *<SPI>*	Specifies encapsulating security payload protocol.
cipher *<keyvalue>*	Specifies encryption/decryption key.
authenticator *<keyvalue>*	Specifies authentication key.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

The inbound local security parameter index (SPI) must equal the outbound remote SPI. The outbound local SPI must equal the inbound remote SPI. The key values are the hexadecimal representations of the keys. They are not true ASCII strings. Therefore, a key of 3031323334353637 represents "01234567".

See the following list for key length requirements.

Algorithm:	Minimum key length required:
DES	64-bits in length; 8 hexadecimal bytes
3DES	192-bits in length; 24 hexadecimal bytes
AES-128-CBC	128-bits in length; 16 hexadecimal bytes
AES-192-CBC	192-bits in length; 24 hexadecimal bytes
AES-256-CBC	256-bits in length; 32 hexadecimal bytes
MD5	128-bits in length; 16 hexadecimal bytes
SHA1	160-bits in length; 20 hexadecimal bytes

Technology Review

The following example configures an AOS product for VPN using IPSec manual keys. This example assumes that the AOS product has been configured with a WAN IP Address of 63.97.45.57 on interface **ppp 1** and a LAN IP Address of 10.10.10.254 on interface **ethernet 0/1**. The Peer Private IP Subnet is 10.10.20.0.

For more detailed information on VPN configuration, refer to the technical support note *Configuring VPN* located on the ***ADTRAN OS Documentation*** CD provided with your unit.

Step 1:

Enter the Global Configuration mode (i.e., config terminal mode).

```
>enable
#configure terminal
```

Step 2:

Enable VPN support using the **ip crypto** command. This command allows crypto maps to be applied to interfaces, and enables the IKE server to listen for IKE negotiation sessions on UDP port 500.

```
(config)#ip crypto
```

Step 3:

Define the transform set. A transform set defines the encryption and/or authentication algorithms to be used to secure the data transmitted over the VPN tunnel. Multiple transform sets may be defined in a system. Once a transform set is defined, many different crypto maps within the system can reference it. In this example, a transform set named **highly_secure** has been created. This transform set defines ESP with authentication implemented using 3DES encryption and SHA1 authentication.

```
(config)#crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac
(cfg-crypto-trans)#mode tunnel
```

Step 4:

Define an IP access list. An Extended Access Control List is used to specify which traffic needs to be sent securely over the VPN tunnel. The entries in the list are defined with respect to the local system. The source IP address will be the source of the traffic to be encrypted. The destination IP address will be the receiver of the data on the other side of the VPN tunnel.

```
(config)#ip access-list extended corporate_traffic
(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 log
  deny ip any any
```

Step 5:

Create crypto map and define manual keys. A crypto map is used to define a set of encryption schemes to be used for a given interface. A crypto map entry has a unique index within the crypto map set. The crypto map entry will specify whether IKE is used to generate encryption keys or if manually specified keys will be used. The crypto map entry will also specify who will be terminating the VPN tunnel, as well as which transform set or sets will be used to encrypt and/or authenticate the traffic on that VPN tunnel. It also specifies the lifetime of all created IPSec security associations.

The keys for the algorithms defined in the transform set associated with the crypto map will be defined by using the **set session-key** command. A separate key is needed for both inbound and outbound traffic. The key format consists of a string of hexadecimal values without the leading **0x** for each character. For example, a cipher key of **this is my cipher key** would be entered as:

74686973206973206D7920636970686572206B6579.

A unique Security Parameter Index (SPI) is needed for both inbound and outbound traffic. The local system's inbound SPI and keys will be the peer's outbound SPI and keys. The local system's outbound SPI and keys will be the peer's inbound SPI and keys. In this example the following keys and SPIs are used:

Inbound cipher SPI:	300	Inbound cipher key:	"2te$#g89jnr(j!@4rvnfhg5e"
Outbound cipher SPI:	400	Outbound cipher key:	"8564hgjelrign*&(gnb#1$d3"
Inbound authenticator key:		"r5%^ughembkdhj34$x.<"	
Outbound authenticator key:		"io78*7gner#4(mgnsd!3"	

```
(config)#crypto map corporate_vpn 1 ipsec-ike
(config-crypto-map)#match address corporate_traffic
(config-crypto-map)#set peer 63.105.15.129
(config-crypto-map)#set transform-set highly_secure
(config-crypto-map)#set session-key inbound esp 300 cipher
32746524236738396A6E72286A21403472766E6668673565 authenticator
7235255E756768656D626B64686A333424782E3C
(config-crypto-map)#set session-key outbound esp 400 cipher
3835363468676A656C7269676E2A2628676E622331246433 authenticator
696F37382A37676E65722334286D676E73642133
```

Step 6:

Configure public interface. This process includes configuring the IP address for the interface and applying the appropriate crypto map to the interface. Crypto maps are applied to the interface on which encrypted traffic will be transmitted.

```
(config)#interface ppp 1
(config-ppp 1)#ip address 63.97.45.57 255.255.255.248
(config-ppp 1)#crypto map corporate_vpn
(config-ppp 1)#no shutdown
```

Step 7:

Configure private interface to allow all traffic destined for the VPN tunnel to be routed to the appropriate gateway.

```
(config)#interface ethernet 0/1
(config-eth 0/1)#ip address 10.10.10.254 255.255.255.0
(config-eth 0/1)#no shutdown
(config-eth 0/1)#exit
```

set transform-set *<setname>*

Use the **set transform-set** command to assign a transform set to a crypto map. See *crypto ipsec transform-set <setname> <parameters>* on page 329 for information on defining transform sets.

Syntax Description

<setname>	Assigns a transform set to this crypto map by entering the set name.

Default Values

By default, no transform set is assigned to the crypto map.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Crypto map entries do not directly contain the transform configuration for securing data. Instead, the crypto map is associated with transform sets which contain specific security algorithms (see *crypto ipsec transform-set <setname> <parameters>* on page 329).

If no transform set is configured for a crypto map, then the entry is incomplete and will have no effect on the system. For manual key crypto maps, only one transform set can be specified.

Usage Examples

The following example first creates a transform set (**Set1**) consisting of two security algorithms (up to three may be defined), and then assigns the transform set to a crypto map (**Map1**):

```
(config)#crypto ipsec transform-set Set1 esp-3des esp-sha-hmac
(cfg-crypto-trans)#exit

(config)#crypto map Map1 1 ipsec-manual
(config-crypto-map)#set transform-set Set1
```

IKE CLIENT COMMAND SET

To activate the IKE Client mode, enter the **crypto ike client** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ike client configuration pool ConfigPool1
(config-ike-client-pool)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

dns-server <address1> <address2> on page 1064

ip-range <start ip> <end ip> on page 1065

netbios-name-server <address1> <address2> on page 1066

NOTE *For VPN configuration example scripts, refer to the technical support note **Configuring VPN** located on the **ADTRAN OS Documentation** CD provided with your unit.*

dns-server *<address1> <address2>*

Use the **dns-server** command to specify the DNS server address(es) to assign to a client.

Syntax Description

<address1>	Assigns the first DNS server address.
<address2>	Optional. Assigns the second DNS server address.

Default Values

By default, no DNS server address is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example defines two DNS server addresses for this configuration pool:

```
(config)#crypto ike client configuration pool ConfigPool1
(config-ike-client-pool)#dns-server 172.1.17.1 172.1.17.3
```

ip-range *<start ip> <end ip>*

Use the **ip-range** command to specify the range of addresses from which the router draws when assigning an IP address to a client.

Syntax Description

<start ip>	Specifies the first IP address in the range for this pool.
<end ip>	Specifies the last IP address in the range for this pool.

Default Values

By default, no IP address range is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example defines an IP address range for this configuration pool:

```
(config)#crypto ike client configuration pool ConfigPool1
(config-ike-client-pool)#ip-range 172.1.1.1 172.1.1.25
```

netbios-name-server *<address1> <address2>*

Use the **netbios-name-server** command to specify the NetBIOS Windows Internet Naming Service (WINS) name servers to assign to a client.

Syntax Description

<address1>	Specifies the first WINs server address to assign.
<address2>	Specifies the second WINs server address to assign.

Default Values

By default, no WINs server address is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example defines two WINs server addresses for this configuration pool:

```
(config)#crypto ike client configuration pool ConfigPool1
(config-ike-client-pool)#netbios-name-server 172.1.17.1 172.1.17.25
```

IKE Policy Attributes Command Set

To activate the IKE Policy Attributes mode, enter the **attribute** command at the IKE Policy prompt. For example:

```
>enable
#configure terminal
(config)#crypto ike policy 1
(config-ike)#attribute 10
(config-ike-attribute)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

authentication [dss-sig | pre-share | rsa-sig] on page 1068

encryption [aes-xxx-cbc | des | 3des] on page 1069

group [1 | 2] on page 1070

hash [md5| sha] on page 1071

lifetime <seconds> on page 1072

NOTE *For VPN configuration example scripts, refer to the technical support note **Configuring VPN** located on the **ADTRAN OS Documentation** CD provided with your unit.*

authentication [dss-sig | pre-share | rsa-sig]

Use the **authentication** command to configure this IKE policy's use of pre-shared secrets and signed certificates during IKE negotiation.

Syntax Description

dss-sig	Specifies to use DSS-signed certificates during IKE negotiation to validate the peer.
pre-share	Specifies the use of pre-shared secrets during IKE negotiation to validate the peer.
rsa-sig	Specifies to use RSA-signed certificates during IKE negotiation to validate the peer.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.
Release 5.1	Command was expanded to include signed certificates.

Functional Notes

Both sides must share the same pre-shared secret in order for the negotiation to be successful.

Usage Example

The following example enables preshared secrets for this IKE policy:

```
(config-ike)#attribute 10
(config-ike-attribute)#authentication pre-share
```

encryption [aes-xxx-cbc | des | 3des]

Use the **encryption** command to specify which encryption algorithm this IKE policy will use to transmit data over the IKE-generated SA.

Syntax Description

aes-128-cbc	Specifies the AES-128-CBC encryption algorithm.
aes-192-cbc	Specifies the AES-192-CBC encryption algorithm.
aes-256-cbc	Specifies the AES-256-CBC encryption algorithm.
des	Specifies the DES encryption algorithm.
3des	Specifies the 3DES encryption algorithm.

Default Values

By default, encryption is set to DES.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example selects 3DES as the encryption algorithm for this IKE policy:

```
(config-ike)#attribute 10
(config-ike-attribute)#encryption 3des
```

group [1 | 2]

Use the **group** command to specify the Diffie-Hellman Group (1 or 2) to be used by this IKE policy to generate the keys (which are then used to create the IPSec SA).

Syntax Description

1	Specifies 768-bit mod P.
2	Specifies1024-bit mod P.

Default Values

By default, group is set to 1.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

The local IKE policy and the peer IKE policy must have matching group settings in order for negotiation to be successful.

Usage Examples

The following example sets this IKE policy to use Diffie-Hellman Group 2:

```
(config-ike)#attribute 10
(config-ike-attribute)#group 2
```

hash [md5| sha]

Use the **hash** command to specify the hash algorithm to be used to authenticate the data transmitted over the IKE SA.

Syntax Description

md5	Choose the MD5 hash algorithm.
sha	Choose the SHA hash algorithm.

Default Values

By default, hash is set to **sha**.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example specifies **md5** as the hash algorithm:

```
(config-ike)#attribute 10
(config-ike-attribute)#hash md5
```

lifetime *<seconds>*

Use the **lifetime** command to specify how long an IKE SA is valid before expiring.

Syntax Description

<seconds>	Specify how many seconds an IKE SA will last before expiring.

Default Values

By default, lifetime is set to 28,800 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series units.

Command History

Release 4.1	Command was introduced.

Usage Examples

The following example sets a lifetime of two hours:

```
(config-ike)#attribute 10
(config-ike-attribute)#lifetime 7200
```

IKE POLICY COMMAND SET

To activate the IKE Policy mode, enter the **crypto ike policy** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#crypto ike policy 1
(config-ike)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

attribute <policynumber> on page 1074

client authentication host on page 1075

client authentication host xauth-type [generic | otp | radius] on page 1076

client authentication server list <listname> on page 1077

client configuration pool <poolname> on page 1078

initiate [main | aggressive] on page 1079

local-id [address | asn1-dn | fqdn | user-fqdn] <ipaddress or name> on page 1080

nat-traversal <version> [allow | disable | force] on page 1082

peer [<ip address> | any] on page 1083

respond [main | aggressive | anymode] on page 1085

> NOTE
>
> *For VPN configuration example scripts, refer to the technical support note **Configuring VPN** located on the **ADTRAN OS Documentation** CD provided with your unit.*

attribute *<policynumber>*

Use the **attribute** command to define attributes for the associated IKE policy. Multiple attributes can be created for a single IKE policy. Once you enter this command, you are in the IKE Policy Attribute mode. Refer to *IKE Policy Attributes Command Set* on page 1067 for more information.

Syntax Description

<policynumber>	Assigns a number (range: 1 to 65,535) to the attribute policy. The number is the attribute's priority number and specifies the order in which the resulting VPN proposals get sent to the far end. This command takes you to the **(config-ike-attribute)#** prompt. From here, you can configure the settings for the attribute as outlined in the section *IKE Policy Attributes Command Set* on page 1067.

Default Values

By default, no attribute is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

Multiple attributes on an IKE policy are ordered by number (with the lowest number representing the highest priority).

Usage Examples

The following example defines a policy attribute (**10**) and takes you into the IKE Policy Attributes:

```
(config-ike)#attribute 10
(config-ike-attribute)#
```

client authentication host

Use the **client authentication host** command to enable the unit to act as an Xauth host when this IKE policy is negotiated with a peer.

Variations of this command include the following:

client authentication host username <*username*>
client authentication host username <*username*> **password** <*word*>
client authentication host username <*username*> **password** <*word*> **passphrase** <*phrase*>

Syntax Description

username <*username*>	Specifies the value sent via Xauth as the username.
password <*word*>	Specifies the value sent via Xauth as the password.
passphrase <*phrase*>	Optional. Specifies the value sent via Xauth as the passphrase. This is only used with authentication type OTP (one time password).

Default Values

By default, if this command is not present in the IKE policy the unit does not act as an Xauth host.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

The specified credentials are programmed into the unit and there is no prompt for entering values real-time. Therefore, schemes requiring real-time input or additional responses (e.g., SecureID) are not supported. The **client authentication host** command and the **client authentication server** commands are mutually exclusive. Refer to *client authentication server list <listname>* on page 1077 for more information.

Usage Examples

The following example specifies the login credentials to be sent:

```
(config-ike)#client authentication host username jsmith password password1 passphrase phrase
```

client authentication host xauth-type [generic | otp | radius]

Use the **client authentication host xauth-type** command to allow the user to specify the Xauth authentication type if a type other than **generic** is desired.

Syntax Description

generic	Specifies generic authentication type.
otp	Specifies OTP authentication type.
radius	Specifies RADIUS authentication type.

Default Values

By default, this is set to generic.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

This command is used along with the **client authentication host username**. Refer to *client configuration pool <poolname>* on page 1078 for more information. When acting as an Xauth host, this command allows the user to specify the Xauth authentication type if a type other than generic is desired.

Usage Examples

The following example sets the Xauth type to **radius**:

```
(config-ike)#client authentication host xauth-type radius
```

client authentication server list *<listname>*

Use the **client authentication server list** command to enable the unit to act as an Xauth server (edge device).

Syntax Description

<listname>	Specifies the named list created with the **aaa authentication login** command.

Default Values

By default, the router does not act as an Xauth server and extended authentication is not performed.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Functional Notes

When this IKE policy is negotiated and the peer has indicated Xauth via the IKE authentication method and/or the Xauth vendor ID, this command allows the unit to perform as an Xauth server (edge device). The specified AAA login method is used to identify the location of the user authentication database. The **client authentication host** and the **client authentication server** commands are mutually exclusive. Refer to *client configuration pool <poolname>* on page 1078 for more information.

Usage Examples

The following example enables Xauth as an Xauth server and specifies which AAA method list to use in locating the user database:

```
(config-ike)#client authentication server list clientusers
```

client configuration pool *<poolname>*

Use the **client configuration pool** command to configure the AOS to perform as mode-config server (edge device) when an IKE policy is negotiated.

Variations of this command include the following:

client configuration pool *<poolname>*
client configuration pool *<poolname>* **initiate**
client configuration pool *<poolname>* **initiate respond**
client configuration pool *<poolname>* **respond**
client configuration pool *<poolname>* **respond initiate**

Syntax Description

<poolname>	The pool from which to obtain parameters to assign to the client.

Default Values

By default, if this command is not present in the IKE policy, the ADTRAN device allocates mode-config IP addresses, DNS server addresses, and NetBIOS name server addresses, and mode-config is not performed.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

This command ties an existing client configuration pool to an IKE policy.

Usage Examples

The following example ties the **ConfigPool1** configuration pool to this IKE policy:

```
(config-ike)#client configuration pool ConfigPool
```

initiate [main | aggressive]

Use the **initiate** command to allow the IKE policy to initiate negotiation (in main mode or aggressive mode) with peers. Use the **no** form of this command to allow the policy to respond only.

Syntax Description

main	Specifies to initiate using main mode. Main mode requires that each end of the VPN tunnel has a static WAN IP address. Main mode is more secure than aggressive mode because more of the main mode negotiations are encrypted.
aggressive	Specifies to initiate using aggressive mode. Aggressive mode can be used when one end of the VPN tunnel has a dynamically assigned address. The side with the dynamic address must be the initiator of the traffic and tunnel. The side with the static address must be the responder.

Default Values

By default, the **main** initiation mode is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

By using the **initiate** and **respond** commands, you can configure the IKE policy to initiate and respond, initiate only, or respond only. It is an error if you have both **initiate** and **respond** disabled.

Usage Examples

The following example enables the AOS device to initiate IKE negotiation in main mode:

```
(config-ike)#initiate main
```

local-id [address | asn1-dn | fqdn | user-fqdn] *<ipaddress or name>*

Use the **local-id** command to set the local ID for the IKE policy. This setting overrides the system local ID setting (set in the Global Configuration mode using the **crypto ike local-id address** command).

Syntax Description

address *<ipaddress>*	Specifies a remote ID of IPv4 type.
asn1-dn *<name>*	Specifies an Abstract Syntax Notation Distinguished Name as the remote ID (enter this value in LDAP format).
fqdn <name>	Specifies a fully qualified domain name (e.g., adtran.com) as the remote ID.
user-fqdn <name>	Specifies a user fully qualified domain name or email address (e.g., user1@adtran.com) as the remote ID.

Default Values

By default, the local ID is not defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

The local ID for a particular IKE policy can be set in two ways. The first (default) method is done in the Global Configuration mode:

(config)#**crypto ike local-id address**

This command, which by default is executed on start-up, makes the local ID of an IKE policy equal to the IPv4 address of the interface on which an IKE negotiation is occurring. This is particularly useful for products that could have multiple public interfaces.

The second method is to use the IKE policy command:
(config-ike)#**local-id [address | fqdn | user-fqdn]** *<ipaddress or fqdn>*

This policy-specific command allows you to manually set the local ID for an IKE policy on a per-policy basis. You can use both methods simultaneously in the product. Several IKE policies can be created, some of which use the default system setting of the IPv4 address of the public interface. Others can be set to override this system setting and manually configure a local ID specific to those policies. When a new IKE policy is created, they default to **no local-id**. This allows the system local ID setting to be applied to the policy.

Usage Examples

The following example sets the local ID of this IKE policy to the IPv4 address 63.97.45.57:

```
(config-ike)#local-id address 63.97.45.57
```

nat-traversal *<version>* [allow | disable | force]

Use the **nat-traversal** command to allow, force, or disable NAT traversal version 1 and 2 on a specific Ike policy.

Syntax Description

<version>	Specifies **v1** or **v2** to select the NAT traversal version.
allow	Sets the IKE policy to allow the specified NAT traversal version.
disable	Sets the IKE policy to disable the specified NAT traversal version.
force	Sets the IKE policy to force the specified NAT traversal version.

Default Values

The defaults for this command are **nat-traversal v1 allow** and **nat-traversal v2 allow**.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 7.1	Command was introduced.

Usage Examples

The following example disables version 2 on Ike policy 1:

```
(config)#crypto ike policy 1
(config-ike)#nat-traversal v2 disable
```

peer [*<ip address>* | any]

Use the **peer** command to enter the IP address of the peer device. Repeat this command for multiple peers. Use the **any** keyword if you want to set up a policy that will initiate or respond to any peer.

Syntax Description

<ip address>	Specifies a peer IP address.
any	Allows any peer to connect to this IKE policy.

Default Values

There are no default settings for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

An IKE policy is incomplete unless one of the peer commands is specified. Only one IKE policy can be configured with **peer any**.

Usage Examples

The following example sets multiple peers on an IKE policy for an initiate-and-respond policy using pre-shared secret, DES, MD5, and Diffie-Hellman Group 1:

```
(config)#crypto ike policy 100
(config-ike)#peer 63.97.45.57
(config-ike)#peer 63.105.15.129
(config-ike)#peer 192.168.1.3
(config-ike)#respond anymode
(config-ike)#initiate main
```

The following example sets up a policy allowing any peer to initiate using preshared secret, DES, MD5, and Diffie-Hellman Group 1.

```
(config)#crypto ike policy 100
(config-ike)#peer any
(config-ike)#respond anymode
(config-ike)#initiate main
```

Technology Review

IKE policies must have a peer address associated with them to allow certain peers to negotiate with the ADTRAN product. This is a problem when you have “roaming” users (those who obtain their IP address using DHCP or some other dynamic means). To allow for “roaming” users, the IKE policy can be set up with **peer any** to allow any peer to negotiate with the ADTRAN product. There can only be one **peer any** policy in the running configuration.

respond [main | aggressive | anymode]

Use the **respond** command to allow the IKE policy to respond to negotiations by a peer. Use the **no** form of this command to allow the policy to only initiate negotiations.

Syntax Description

main	Specifies to respond only to main mode.
aggressive	Specifies to respond only to aggressive mode.
anymode	Specifies to respond to any mode.

Default Values

By default, respond to any mode is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 4.1	Command was introduced.

Functional Notes

By using the **initiate** and **respond** commands, you can configure the IKE policy to initiate and respond, initiate only, or respond only. It is an error if you have both **initiate** and **respond** disabled.

Usage Examples

The following example configures the router to initiate and respond to IKE negotiations:

```
(config-ike)#respond anymode
(config-ike)#initiate main
```

AS PATH LIST COMMAND SET

To activate the Autonomous System (AS) Path List Configuration mode, enter the **ip as-path-list** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip as-class-list listname
(config-as-path-list)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

All other commands for this command set are described in this section in alphabetical order.

deny on page 1087

permit on page 1088

deny

Use the **deny** command to deny a BGP route that matches the as-path attributes.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example denies BGP routes that match as-path attributes:

```
(config)#ip as-path-list listname
(config-as-path-list)#deny
```

permit

Use the **permit** command to allow a BGP route that matches the as-path attributes.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example permits BGP routes that match the as-path attributes:

```
(config)#ip as-path-list listname
(config-as-path-list)#permit
```

BGP Configuration Command Set

To activate the BGP Configuration mode, enter the **router bgp** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router bgp 1
(config-bgp)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

All other commands for this command set are described in this section in alphabetical order.

bgp fast-external-fallover on page 1090

bgp log-neighbor-changes on page 1091

bgp router-id <ip address> on page 1092

distance bgp <external> <internal> <local> on page 1093

hold-timer <hold time> on page 1094

bgp fast-external-fallover

Use the **bgp fast-external-fallover** command to enable the fast-external-fallover feature.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

When enabled, if the link interface over which the router is communicating with a BGP peer goes down, the BGP session with that peer is immediately cleared. When fallover is disabled and the link goes down, the session is maintained until the BGP hold timer expires.

Usage Examples

The following example enables this option:

```
(config)#router bgp 1
(config-bgp)#bgp fast-external-fallover
```

bgp log-neighbor-changes

Use the **bgp log-neighbor-changes** command to control the logging of neighbor state changes. Use the **no** form of this command to return to the default setting.

Syntax Description

No subcommands.

Default Values

By default, neighbor changes are not logged.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command controls logging of BGP neighbor state changes (up/down) and resets. This information is useful for troubleshooting and determining network stability.

Usage Examples

The following example enables logging of BGP neighbor state changes:

```
(config)#router bgp 1
(config-bgp)#bgp log-neighbor-changes
```

bgp router-id *<ip address>*

Use the **bgp router-id** command to specify the IP address that the router should use as its BGP router ID. Use the **no** form of this command to return to the default setting.

Syntax Description

<ip address>	Designates the IP address this router should use as its BGP router ID.

Default Values

By default, no router ID is configured. The default action is detailed in *Functional Notes*, below.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command allows an IP address to be specified for use as the BGP router ID. If no IP address is configured at BGP startup, it uses the highest IP address configured on a loopback interface. If no loopback interfaces are configured, it uses the highest IP address configured on any interface that is active. If the specified router ID is changed, existing sessions with BGP neighbors are reset.

Usage Examples

The following example configures IP address 10.0.0.1 as the BGP router ID:

```
(config)#router bgp 1
(config-bgp)#bgp router-id 10.0.0.1
```

distance bgp *<external> <internal> <local>*

Use the **distance bgp** command to set the administrative distance for BGP routes. Use the **no** form of this command to return to the default setting.

Syntax Description

<external>	Sets the administrative distance for BGP routes learned via eBGP sessions. A value of 255 means the route is not installed. Range: 1 to 254.
<internal>	Sets the administrative distance for BGP routes learned via iBGP sessions. A value of 255 means the route is not installed. Range: 1 to 254.
<local>	Sets the administrative distance for BGP routes learned via the network command and redistribution. A value of 255 means the route is not installed. Range: 1 to 254.

Default Values

By default external is set to 20, internal to 200, and local to 200. Normally, these default settings should not be changed.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command sets the administrative distance for BGP routes. The administrative distance is a local variable that allows a router to choose the best route when there are multiple paths to the same network. Routes with smaller administrative distances are favored.

Usage Examples

The following example gives external BGP routes an administrative distance of 30, internal BGP routes an administrative distance of 200, and local routes an administrative distance of 240:

```
(config)#router bgp 1
(config-bgp)#distance bgp 30 200 240
```

hold-timer *<hold time>*

Use the **hold-timer** command to set the default hold time for all neighbors in the BGP process.

Syntax Description

<hold time>	Specifies a time interval (in seconds) within which a keepalive must be received from a peer before it is declared dead peer. Range: 0 to 65,535

Default Values

By default, the hold time is 90 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

Using the **hold-timer** command in BGP configuration mode sets the default hold time for all neighbors in that BGP process. Using the **hold-timer** command in BGP neighbor configuration mode sets the hold time for only that neighbor. The peers will negotiate and use the lowest configured setting. The keepalive interval will be set to one third of the negotiated hold time.

Usage Examples

The following example sets a hold time of 120 seconds for a specific neighbor, with an understood keepalive interval of 40 seconds:

```
(config)#router bgp 1
(config-bgp)#hold-timer 120
```

BGP NEIGHBOR CONFIGURATION COMMAND SET

To activate the BGP Neighbor Configuration mode, enter the **router bgp-neighbor** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

access-list <listname> [in | out] on page 1096

advertisement-interval <seconds> on page 1097

as-path-list <listname> [in | out] on page 1098

ebgp-multihop <hop count> on page 1099

hold-timer <hold time> on page 1100

local-as <as-number> on page 1101

next-hop-self on page 1103

password <password> on page 1104

prefix-list <listname> [in | out] on page 1105

remote-as <as-number> on page 1106

route-map <map-name> [in | out] on page 1107

send-community standard on page 1108

soft-reconfiguration inbound on page 1109

update-source <interface> on page 1110

access-list *<listname>* [in | out]

Use the **access-list** command to assign a predefined access list to a BGP neighbor. This list is then used to filter inbound and/or outbound BGP route updates. Use the **no** form of this command to return to default settings.

Syntax Description

<listname>	Assigns an access list to this BGP neighbor.
in	Specifies the filtering of all inbound BGP route updates.
out	Specifies the filtering of all outbound BGP route updates.

Default Values

By default, no access lists are specified for filtering.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

Before they can be assigned to a neighbor, access lists must first be defined using the **ip access-list** commands. See *ip access-list extended <listname>* on page 344 and *ip access-list standard <listname> [permit | deny] <ip address>* on page 350 for more information.

Usage Examples

The following example uses the **InWeb** access list to filter all inbound BGP route updates:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#access-list InWeb in
```

advertisement-interval *<seconds>*

Use the **advertisement-interval** command to configure the AOS to specify how long the BGP process waits before sending updates to the neighbor.

Syntax Description

<seconds>	Specifies the advertisement interval in seconds. Range: 0 to 600.

Default Values

By default, the advertisement interval is 30 seconds for external neighbors and 5 seconds for internal neighbors.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command sets the minimum interval between sending updates to the specified neighbor.

Usage Examples

The following example configures the BGP process to wait at least 100 seconds before sending updates to the neighbor:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#advertisement-interval 100
```

as-path-list *<listname>* [in | out]

Use the **as-path-list** command to assign a predefined autonomous system (AS) path list to a BGP neighbor. This list is then used to filter inbound and/or outbound BGP route updates. Use the **no** form of this command to discontinue use of the list.

Syntax Description

<listname>	Assigns an AS path list to this BGP neighbor.
in	Specifies the filtering of all inbound BGP route updates.
out	Specifies the filtering of all outbound BGP route updates.

Default Values

By default, no AS path lists are specified for filtering.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

Before they can be assigned to a neighbor, AS path lists must first be defined using the **ip as-path-list** command.

Usage Examples

The following example uses the **no15** AS path list to filter all inbound BGP route updates:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#as-path-list no15 in
```

ebgp-multihop *<hop count>*

Use the **ebgp-multihop** command to configure the maximum hop count of BGP messages to a neighbor. Use the **no** form of this command to return to the default setting.

Syntax Description

<hop count>	Specifies the maximum hop count of BGP messages to a neighbor. Range: 1 to 254.

Default Values

By default, eBGP multihop is set to 1.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

This command allows an eBGP neighbor to be on a network that is not directly connected. Normally, eBGP peers are directly connected. In certain applications, a non-BGP device such as a firewall or router may reside between eBGP peers. In this case, the eBGP multihop command is required to allow updates to have a TTL greater than 1 and to allow received BGP updates to be added to the BGP table when the next hop address is not directly connected.

Usage Examples

The following example allows a BGP message to travel 10 hops to a neighbor:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#ebgp-multihop 10
```

hold-timer *<hold time>*

Use the **hold-timer** command to set the default hold time for all neighbors in the BGP process.

Syntax Description

<hold time>	Specifies a time interval (in seconds) within which a keepalive must be received from a peer before it is declared dead peer. Range: 0 to 65,535.

Default Values

By default, the hold time is 90 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 8.1	Command was introduced.

Functional Notes

Using the **hold-timer** command in BGP configuration mode sets the default hold time for all neighbors in that BGP process. Using the **hold-timer** command in BGP neighbor configuration mode sets the hold time for only that neighbor. The peers will negotiate and use the lowest configured setting. The keepalive interval will be set to one-third of the negotiated hold time.

Usage Examples

The following example sets a hold time of 120 seconds for a specific neighbor, with an understood keepalive interval of 40 seconds:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#hold-timer 120
```

local-as *<as-number>*

Use the **local-as** command to specify an autonomous system (AS) number for the unit to use when communicating with this BGP neighbor. Use the **no** form of this command to return to default settings.

Syntax Description

<as-number>	Specifies the AS number to use when communicating with this neighbor. Must be different than the AS number for this router and the peer router. Only valid for eBGP connections. Range is 0 to 65,535.

Default Values

By default, no local AS number is defined. The router's BGP AS number is used.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

This command substitutes a different AS number to be used for communicating with this BGP neighbor. (other than the one the router is actually a member of). This can be used to satisfy network designs requiring a customer to appear as one AS number when communicating with one internet service provider (ISP) and another when communicating with another ISP.

Usage Examples

The following example configures this BGP neighbor's AS number to be **300**:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#local-as 300
```

Technology Review

This router appears (to the peer router) to be in the AS specified with the **local-as** command. Therefore all routes learned from the peer have this number prepended to the AS path. In network advertisements from routers using the **local-as** command, the router's true AS number (the number specified using the **router bgp as-number** command) is prepended to the AS path attribute, and the local-AS (the number specified in the **neighbor local-as** command) is prepended to the AS path attribute. This makes it appear that the path to the network is first through the local-AS, and then through the true AS. To further illustrate, consider the following example network.

In this network:

- Router A is in AS 100.
- Router B is in AS 300.
- Router A is an eBGP peer with Router B.
- Router A’s connection to Router B specifies a **local-as** of 200.
- Router B is configured to connect to Router A in AS 200.

Therefore:

- To Router B, all aspects of Router A appear as AS 200.
- Networks advertised from Router A to Router B will have the AS path **200 100** prepended to the AS path attribute.
- Router A will add AS 200 to the AS path of networks learned from Router B.

next-hop-self

Use the **next-hop-self** command to force the next hop attribute to be changed to this unit's address when advertising networks that would not have the next hop changed under normal rules. Normal next hop rules are described in the *Functional Notes* section below. Use the **no** form of this command to cause normal next hop rules to apply.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled and normal next hop rules apply.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

In eBGP, routes are normally advertised with a next hop set to the IP address that the receiving peer has configured in its neighbor statement for this router. In the eBGP case where the receiving router is in the same subnet as the current next hop, the current next hop is not changed.

For broadcast multiaccess networks (Ethernet), this provides more efficient routing. For non-broadcast multiaccess networks (NBMA) such as Frame Relay with a partial mesh using point-to-multipoint circuits, this rule can cause significant problems. Since the partial mesh is on the same subnet, BGP applies the rule of not changing the next hop address, rendering invalid routes in certain topologies. This is one case where this command is necessary to solve a problem.

Usage Examples

The following example enables **next-hop-self**:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#next-hop-self
```

password *<password>*

Use the **password** command to enable MD5 password authentication on TCP. Use the **no** form of this command to disable authentication.

Syntax Description

<password>	Specifies the password string to be used for authentication. The password is case-sensitive and must not exceed 80 characters.

Default Values

By default, authentication is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

Authentication must be configured on both peers using the same password. Every BGP TCP segment sent is authenticated. Configuring authentication causes an existing session to be torn down and re-established using the currently specified authentication.

Usage Examples

The following example enables authentication for this BGP neighbor and sets a password of **user1**:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#password user1
```

prefix-list *<listname>* [in | out]

Use the **prefix-list** command to assign a predefined prefix list to a BGP neighbor. The list is then used to filter BGP route updates received and/or sent from/by the specified peer. Use the **no** form of this command to discontinue use of the prefix list.

Syntax Description

<listname>	Assigns a prefix list to this BGP neighbor.
in	Specifies the filtering of all inbound BGP route updates received from the specified peer.
out	Specifies the filtering of all outbound BGP route updates being sent to the specified peer.

Default Values

By default, no prefix lists are specified for filtering.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

Before they can be assigned to a BGP neighbor, prefix lists must first be defined using the **ip prefix-list** command. See *ip prefix-list <listname> description <"text">* on page 397 for more information.

Usage Examples

The following example uses the **MyList** prefix list to filter all BGP updates received from the specified peer:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#prefix-list MyList in
```

remote-as *<as-number>*

Use the **remote-as** command to specify the BGP autonomous system (AS) to which the neighbor belongs, adding an entry to the BGP neighbor table. Use the **no** form of this command to return to default settings.

Syntax Description

<as-number>	Specifies the AS number. This number must be different from the AS number of the local router (which is defined using the **router bgp** command). Range: 1 to 65,535. See *router bgp* on page 440 for more information.

Default Values

By default, no BGP neighbors are defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example configures a remote AS number of **200** for this neighbor:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#remote-as 200
```

route-map *<map-name>* [in | out]

Use the **route-map** command to assign a route map to this BGP neighbor. The route map is then used to filter or modify inbound and/or outbound BGP route updates. Use the **no** form of this command to return to default settings.

Syntax Description

<map-name>	Assigns a route map to this BGP neighbor.
in	Specifies the filtering/modification of all inbound BGP route updates.
out	Specifies the filtering/modification of all outbound BGP route updates.

Default Values

By default, no route map is assigned.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

Before a route map can be assigned to a BGP neighbor, it must first be defined using the **route-map** command. See *route-map <map-name> [permit | deny] <sequence number>* on page 439 for more information.

Usage Examples

The following example assigns a route map to this neighbor for outbound filtering:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#route-map MapName out
```

send-community standard

Use the **send-community standard** command to insert a standard BGP community attribute to all outgoing route updates for this neighbor. Use the **no** form of this command to return to default settings.

Syntax Description

No subcommands.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example inserts a standard BGP community attribute to all outgoing route updates for the specified neighbor:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#send-community standard
```

soft-reconfiguration inbound

Use the **soft-reconfiguration inbound** command to enable this unit to store BGP updates for the specified neighbor. Use the **no** form of this command to return to default settings.

Syntax Description

No subcommands.

Default Values

By default, this command is enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

BGP updates are stored prior to filtering, thus allowing the **clear ip bgp soft** command to be used in the absence of route refresh (RFC2918) capability. This command affects all neighbors. See *clear ip bgp [* | <as-number> | <ip address>] [in | out | soft]* on page 50 for more information.

Usage Examples

The following example enables the unit to store BGP updates for the specified neighbor:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#soft-reconfiguration inbound
```

update-source *<interface>*

Use the **update-source** command to specify which virtual interface’s IP address will be used as the source IP address for the BGP TCP connection (when connecting to this peer). Use the **no** form of this command to return to default settings.

Syntax Description

<interface>	Specifies the interface ID (e.g., **loopback 1**) of the virtual interface to be used as the source IP address.

Default Values

By default, the outbound interface's IP address is used for BGP updates.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Functional Notes

This is most often configured as a loopback interface that is reachable by the peer router. The peer will specify this address in its neighbor commands for this router.

Usage Examples

The following example configures the **loopback 1** interface as the source IP:

```
(config)#router bgp-neighbor 192.22.73.101
(config-bgp-neighbor)#update-source loopback 1
```

COMMUNITY LIST COMMAND SET

To activate the Community List Configuration mode, enter the **ip community-list** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip community-list listname
(config-comm-list)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

All other commands for this command set are described in this section in alphabetical order.

deny on page 1112

permit on page 1113

deny

Use the **deny** command to deny a BGP route that matches the community number.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example denies BGP routes that match community numbers:

```
(config)#ip as-path-list listname
(config-comm-list)#deny
```

permit

Use the **permit** command to allow a BGP route that matches the community numbers.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.3	Command was introduced.

Usage Examples

The following example permits BGP routes that match the community numbers:

```
(config)#ip as-path-list listname
(config-comm-list)#permit
```

ROUTER (OSPF) CONFIGURATION COMMAND SET

To activate the Router (OSPF) Configuration mode, enter the **router ospf** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router ospf
(config-ospf)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 32

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

area <area id> default-cost <value> on page 1115

area <area id> range <ip address> <network mask> [advertise | not-advertise] on page 1116

area <area id> stub [no-summary] on page 1117

auto-cost reference-bandwidth <rate> on page 1118

default-information-originate [always | metric <value> | metric-type <type>] on page 1119

default-metric <value> on page 1120

maximum paths <number> on page 1121

network <ip address> <wildcard> area <area id> on page 1122

redistribute connected [metric <value> | metric-type <type> | subnets] on page 1123

redistribute rip [metric <value> | metric-type <type> | subnets] on page 1124

redistribute static [metric <value> | metric-type <type> | subnets] on page 1125

summary-address <address> <mask | prefix mask> not-advertise on page 1126

timers lsa-group-pacing <seconds> on page 1127

timers spf <delay> <hold> on page 1128

area *<area id>* **default-cost** *<value>*

Use the **area default-cost** command to assign a cost of the default summary route sent into a stub area or not-so-stubby-area (NSSA). Use the **no** form of this command to delete the assigned cost.

Syntax Description

<area id>	Specifies the identifier for this area. Specifies as an integer (range: 0 to 4,294,967,295) or an IP address *<A.B.C.D>*.
<value>	Specifies the default summary route cost. Range: 0 to 166,777,214.

Default Values

By default the summary route cost is set to 0. There is no default for the area ID.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example defines a default cost of 85 to a specific area:

```
(config)#router ospf
(config-ospf)#area 192.22.72.0 default-cost 85
```

area *<area id>* **range** *<ip address> <network mask>* **[advertise | not-advertise]**

Use the **area range** command to configure area route summarizations and to determine whether an address range is advertised to the networks.

Syntax Description

<area id>	Specifies an identifier for this area. Specifies as an integer (range: 0 to 4,294,967,295) or an IP address *<A.B.C.D>*.
<ip address>	Specifies the IP address of the advertised summary route.
<network mask>	Specifies the mask of the advertised summary route.
advertise	Specifies the specified address range will be advertised to other networks.
not-advertise	Specifies the specified address range will not be advertised to other networks.

Default Values

By default, OSPF is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example defines an address range for a specific area that allows the unit to advertise this range to other networks:

```
(config)#router ospf
(config-ospf)#area 11.0.0.0 range 11.0.0.0 255.0.0.0 advertise
```

area *<area id>* stub [no-summary]

Use the **area stub** command to configure an area as a stub area. Use the **no** form of this command to disable stub-designation for areas defined as stubs using this command.

Syntax Description

<area id>	Specifies an identifier for this stub area. Specifies as an integer (range: 0 to 4,294,967,295) or an IP address *<A.B.C.D>*.
no-summary	Optional. Designates the area as a total stub area. No summary link advertisements will be sent by the ABR into the stub area.

Default Values

By default, OSPF is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Technology Review

It is important to coordinate configuration of all routers and access servers in the stub area. The **area stub** command must be configured for each of those pieces of equipment. Use the **area router configuration** command with the **area default-cost** command to specify the cost of a default internal router sent into a stub area by an ABR. Refer to *area <area id> default-cost <value>* on page 1115 for related information.

Usage Examples

The following example configures area 2 as a stub area:

```
(config)#router ospf
(config-ospf)#area 2 stub
```

auto-cost reference-bandwidth *<rate>*

Use the **auto-cost reference-bandwidth** command to assign a different interface cost to an interface. It may be necessary to assign a higher number to high-bandwidth links. This value is used in OSPF metric calculations.

Syntax Description

<rate>	Sets the default reference bandwidth rate (range: 1 to 4,294,967 Mbps).

Default Values

By default, the rate is set to 100.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sets the auto cost reference-bandwidth to 1000 Mbps:

```
(config)#router ospf
(config-ospf)#auto-cost reference-bandwidth 1000
```

default-information-originate [always | metric *<value>* | metric-type *<type>*]

Use the **default-information-originate** command to cause an ASBR to generate a default route. It must have its own default route before it generates one unless the **always** keyword is used.

Syntax Description

always	Optional. Specifies to always advertise default route.
metric *<value>*	Optional. Configures the metric value (range is 0 to 16,777,214).
metric type *<type>*	Optional. Configures the metric type (1 or 2).

Default Values

metric *<value>*	**10**
metric type *<type>*	**2**

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example configures a router to always advertise default routes and assigns the default router a metric value of 10000 and a metric type of 2:

```
(config)#router ospf
(config-ospf)#default-information-originate always metric 10000 metric-type 2
```

default-metric *<value>*

Use the **default-metric** command to set a metric value for redistributed routes.

Syntax Description

<value>	Sets the default metric value (range: 0 to 4,294,967,295).

Default Values

By default, **default-metric** value is set at 20.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The metric value defined using the **redistribute** command overrides the **default-metric** command's metric setting. Refer to *redistribute ospf [metric <value>]* on page 1140 for related information.

Usage Examples

The following example shows a router using both RIP and OSPF routing protocols. The example advertises RIP-derived routes using the OSPF protocol and assigns the RIP-derived routes an OSPF metric of 10.

```
(config)#router ospf
(config-ospf)#default-metric 10
(config-ospf)#redistribute rip
```

maximum paths *<number>*

Use the **maximum paths** command to set the maximum number of multipath routes to advertise to the route table via OSPF.

Syntax Description

<number>	Specifies the number of routes OSPF can insert into the route table. Valid range: 1 to 6.

Default Values

By default, **maximum paths** is set to **4**.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the maximum number of multipath routes OSPF can insert in the route table to 5.

```
(config)#router ospf
(config-ospf)#maximum paths 5
```

network *<ip address> <wildcard>* **area** *<area id>*

Use the **network area** command to enable routing on an IP stack and to define area IDs for the interfaces on which OSPF will run. Use the **no** form of this command to disable OSPF routing for interfaces defined using this command.

Syntax Description

<ip address>	Specifies the network address *<A.B.C.D>*.
<wildcard>	The wildcard mask is in an IP-address-type format and includes "don't care" bits.
<area id>	Specifies an identifier for this area. Specifies as an integer (range: 0 to 4,294,967,295) or an IP address *<A.B.C.D>*.

Default Values

No default values required for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Technology Review

In order for OSPF to operate on an interface, the *primary* address for the interface must be included in the **network area** command. Assigning an interface to an OSPF area is done using the **network area** command. There is no limit to the number of **network area** commands used on a router. If the address ranges defined for different areas overlap, the first area in the **network area** command list is used and all other overlapping portions are disregarded. Try to avoid overlapping to avoid complications.

Usage Examples

In the following example, the OSPF routing process is enabled and two OSPF areas are defined:

```
(config)#router ospf
(config-ospf)#network 192.22.72.101 0.0.0.255 area 0
(config-ospf)#network 10.0.0.0 0.255.255.255 area 10.0.0.0
```

redistribute connected [metric *<value>* | metric-type *<type>* | subnets]

Use the **redistribute connected** command to advertise routes from one protocol to another. Using the **connected** keyword allows the advertisement of connected routes into the OSPF routing protocol. This will advertise all connected routes on OSPF-enabled interfaces. It does not enable OSPF on all interfaces. Use the **no** form of this command to disable the propagation of the specified route type.

Syntax Description

metric *<value>*	Optional. Specifies a metric value to be carried from one OSPF process to the next (if no other value is specified).
metric-type *<type>*	Optional. Specifies a type 1 or type 2 external route as the external link type. If not specified, the default is 2.
subnets	Optional. Specifies subnet redistribution when redistributing routes into OSPF.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 10.1	Subcommands were added.

Functional Notes

Redistributing connected routes imports those routes into OSPF without the interfaces in question actually participating in OSPF. The connected routes imported this way are not covered by a network command and therefore do not send/receive OSPF traffic.

Usage Examples

The following example imports connected routes into OSPF:

```
(config)#router ospf
(config-ospf)#redistribute connected
```

redistribute rip [metric *<value>* | metric-type *<type>* | subnets]

Use the **redistribute rip** command to advertise routes from one protocol to another, regardless of the routing protocol implemented on the routing domain. Using the **rip** keyword allows the propagation of RIP routes into OSPF. Use the **no** form of this command to disable the propagation of the specified route type.

Syntax Description

metric *<value>*	Optional. Specifies a metric value to be carried from one OSPF process to the next (if no other value is specified).
metric-type *<type>*	Optional. Specifies a type 1 or type 2 external route as the external link type. If not specified, the default is 2.
subnets	Optional. Specifies subnet redistribution when redistributing routes into OSPF.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.
Release 10.1	Subcommands were added.

Functional Notes

Redistributing RIP routes imports those routes into OSPF without the interfaces in question actually participating in OSPF. The RIP routes imported this way are not covered by a network command and therefore do not send/receive OSPF traffic.

Usage Examples

The following example imports RIP routes into OSPF:

```
(config)#router ospf
(config-ospf)#redistribute rip
```

redistribute static [metric *<value>* | metric-type *<type>* | subnets]

Use the **redistribute static** command to advertise routes from one protocol to another. Using the **static** keyword allows the advertisement of static routes into the OSPF routing protocol. This will advertise all static routes on OSPF-enabled interfaces. It does not enable OSPF on all interfaces. Use the **no** form of this command to disable the propagation of the specified route type.

Syntax Description

metric *<value>*	Optional. Specifies a metric value to be carried from one OSPF process to the next (if no other value is specified).
metric-type *<type>*	Optional. Specifies a type 1 or type 2 external route as the external link type. If not specified, the default is 2.
subnets	Optional. Specifies subnet redistribution when redistributing routes into OSPF.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.
Release 10.1	Subcommands were added.

Functional Notes

Redistributing static routes imports those routes into OSPF without the interfaces in question actually participating in OSPF. The static routes imported this way are not covered by a network command and therefore do not send/receive OSPF traffic.

Usage Examples

The following example imports static routes into OSPF:

```
(config)#router ospf
(config-ospf)#redistribute static
```

summary-address *<address> <mask* | *prefix mask>* **not-advertise**

Use the **summary-address** command to control address summarization of routes that are redistributed into OSPF from other sources (e.g., RIP-to-OSPF, static-to-OSPF, etc.). The **not-advertise** option causes suppression of routes that match the specified mask/prefix mask pair.

Syntax Description

<address>	Specifies the IP address or Prefix A.B.C.D.
<mask | *prefix mask>*	Routes matching this mask/prefix mask pair will be suppressed if the **not-advertise** command is enabled.
not advertise	Optional. Causes suppression of routes that match the specified mask/prefix mask pair.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example suppresses advertisement of the routes which match the specified address/mask:

```
(config)#router ospf
(config-ospf)#summary-address 11.0.0.0 255.0.0.0 not-advertise
```

timers lsa-group-pacing *<seconds>*

Use the **timers lsa-group-pacing** command to change the link state advertisement (LSA) refresh interval.

Syntax Description

<seconds>	Sets the LSA refresh interval in seconds (range: 10 to 1800).

Default Values

By default, this value is set at 240 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example sets the refresh interval for six minutes:

```
(config)#router ospf
(config-ospf)#timers lsa-group-pacing 360
```

timers spf *<delay> <hold>*

Use the **timers spf** command to configure the shortest path first (SPF) calculation and hold intervals.

Syntax Description

<delay>	Specifies the time in seconds between OSPF's receipt of topology changes and the beginning of SPF calculations.
<hold>	Specifies the time in seconds between consecutive SPF calculations. Range: 10 to 1800 seconds.

Default Values

<delay>	5 seconds
<hold>	10 seconds

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Usage Examples

The following example defines a delay of 10 seconds and a hold-time of 30 seconds:

```
(config)#router ospf
(config-ospf)#timers spf 10 30
```

ROUTER (PIM SPARSE) CONFIGURATION COMMAND SET

To activate the Router (PIM Sparse) Configuration mode, enter the **router pim-sparse** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router pim-sparse
(config-pim-sparse)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

join-prune-msg-interval <seconds> on page 1130

rp-address <ip address> access-group <access-list-name> on page 1131

spt-threshold <packets> infinity on page 1133

join-prune-msg-interval *<seconds>*

Use the **join-prune-msg-interval** command to set a timing rate for PIM sparse join/prune messages.

Syntax Description

<seconds>	Specifies the PIM sparse join/prune message interval. Valid range: 10 to 65534 seconds.

Default Values

By default, the message interval is set to 60 seconds.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and the Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the interval for 50 seconds:

```
(config)#router pim-sparse
(config-pim-sparse)#join-prune-msg-interval 50
```

rp-address *<ip address>* access-group *<access-list-name>*

Use the **rp-address** command to specify a static IP address for the rendezvous point (RP) router. The **access-group** keyword is used to limit the multicast group addresses to which the RP applies.

Syntax Description

<ip address>	Specifies the IP address for the RP.
access-group	Optional. Specifies the access group to which the RP applies.
<access-list-name>	Optional. Specifies the name of the access group.

Default Values

No default necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and the Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

The **access-group** keyword is used to limit the multicast group addresses to which the RP applies. If more than one RP is configured for a given multicast group address, then a hash algorithm determines the appropriate hierarchy (see below). The results of the hash algorithm can be seen with the **show ip pim-sparse rp-map command**.

The hash algorithm is defined in RFC 2117 section 3.7 as follows:

```
For each RP address C(i) in the RP-Set, whose Group-prefix
     covers G, compute a value:

  Value(G,M,C(i))=
  (1103515245 * ((1103515245 * (G&M)+12345) XOR C(i)) + 12345) mod 2^31
```

where M is a hash-mask included in Bootstrap messages.This hash-mask allows a small number of consecutive groups (e.g., 4) to always hash to the same RP. For instance, hierarchically-encoded data can be sent on consecutive group addresses to get the same delay and fate-sharing characteristics.

The candidate with the highest resulting value is then chosen as the RP for that group, and its identity and hash value are stored with the entry created.

Ties between C-RPs having the same hash value, are broken in advantage of the highest address.

Usage Examples

The following example specifies an IP address of 172.22.5.100 for the RP:

```
(config)#router pim-sparse
(config-pim-sparse)#rp-address 172.22.5.100
```

spt-threshold *<packets>* infinity

Use the **spt-threshold** command to change the PIM Sparse Shortest Path Tree (SPT) threshold, which specifies the number of packets the router sends using the rendezvous point (RP) before switching to the SPT.

Syntax Description

<packets>	Specifies the number of packets the routing switch sends using the RP before switching to the SPT. Valid range: 1 to 4294967295.
infinity	Causes all sources to use the shared RP tree.

Default Values

By default, the SPT threshold is set to 1 packet.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 and the Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the SPT threshold at five packets:

```
(config)#router pim-sparse
(config-pim-sparse)#spt-threshold 5
```

ROUTER (RIP) CONFIGURATION COMMAND SET

To activate the Router (RIP) Configuration mode, enter the **router rip** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#router rip
(config-rip)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

auto-summary on page 1135

timeout-timer <seconds> on page 1142

network <address> <subnet mask> on page 1137

passive-interface <interface> on page 1138

redistribute connected [metric <value>] on page 1139

redistribute ospf [metric <value>] on page 1140

redistribute static [metric <value>] on page 1141

timeout-timer <seconds> on page 1142

update-timer <seconds> on page 1143

version [1 | 2] on page 1144

auto-summary

Use the **auto-summary** command to have RIP version 2 summarize subnets to the classful boundaries. Use the **no** form of this command to disable this summarization.

Syntax Description

No subcommands.

Default Values

By default, auto-summary is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

Use this command if you are subdividing a classful network into many subnets and these subnets are to be advertised over a slow link (64k or less) to a router that can only reach the classful network via the router you are configuring.

Usage Examples

The following example configures the router to not automatically summarize network numbers:

```
(config)#router rip
(config-rip)#no auto-summary
```

default-metric *<value>*

Use the **default-metric** command to set the default metric value for the RIP routing protocol. Use the **no** form of this command to return to the default settings.

Syntax Description

<value>	Sets the default metric value (range: 1 to 4,294,967,295 Mbps).

Default Values

By default, this value is set at 0.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

The metric value defined using the **redistribute** command overrides the **default-metric** command’s metric setting. Refer to *redistribute ospf [metric <value>]* on page 1140 for related information.

Usage Examples

The following example shows a router using both RIP and OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the OSPF-derived routes a RIP metric of 10.

```
(config)#router rip
(config-rip)#default-metric 10
(config-rip)#redistribute ospf
```

network *<address> <subnet mask>*

Use the **network** command to enable RIP on the specified network. The AOS will only allow processing (sending and receiving) RIP messages on interfaces with IP addresses that are contained in the networks listed using this command. All RIP messages received on interfaces not listed using this command will be discarded. To allow for receiving and participating in RIP but not for transmitting, use the **passive-interface** command (refer to *passive-interface <interface>* on page 1138). Use the **no** form of this command to remove a network from the list.

Syntax Description

<address>	Specifies the IP address of the network on which RIP will be enabled.
<subnet mask>	Specifies the subnet mask that corresponds to the entered IP address.

Default Values

By default, RIP is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example enables RIP on the 102.22.72.252/30, 192.45.2.0/24, and 10.200.0.0/16 networks:

```
(config)#router rip
(config-rip)#network 102.22.72.252 255.255.255.252
(config-rip)#network 192.45.2.0 255.255.255.0
(config-rip)#network 10.200.0.0 255.255.0.0
```

passive-interface *<interface>*

Use the **passive-interface** command to disable the transmission of routing updates on the specified interface. All routing updates received on that interface will still be processed (and advertised to other interfaces), but no updates will be transmitted to the network connected to the specified interface. Multiple **passive-interface** commands may be used to create a customized list of interfaces. Use the **no** form of this command to enable the transmission of routing updates on an interface.

Syntax Description

<interface>	Specifies the interface that will not transmit routing updates.

Default Values

By default, RIP is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example disables routing updates on the Frame Relay link (labeled 1.17) and the PPP link (labeled 1):

```
(config)#router rip
(config-rip)#passive-interface frame-relay 1.17
(config-rip)#passive-interface ppp 1
```

redistribute connected [metric *<value>*]

Use the **redistribute connected** command to pass routes from one network to another, regardless of the routing protocol implemented on the routing domain. Using the **connected** keyword allows the propagation of routes connected to other interfaces using the RIP routing protocol. Use the **no** form of this command to disable the propagation of the specified route type.

Syntax Description

metric *<value>*	Optional. Specifies the hop count to use for advertising redistributed OSPF routes in RIP.

Default Values

By default, RIP is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

Redistributing connected routes imports those routes into RIP without the interfaces in question actually participating in RIP. The connected routes imported this way are not covered by a network command and therefore do not send/receive RIP traffic.

Usage Examples

The following example passes the connected routes found in the route table to other networks running the RIP routing protocol:

```
(config)#router rip
(config-rip)#redistribute connected
```

redistribute ospf [metric *<value>*]

Use the **redistribute ospf** command to advertise routes from one protocol to another, regardless of the routing protocol implemented on the routing domain. Using the **ospf** keyword allows the propagation of OSPF routes into RIP. Use the **no** form of this command to disable the propagation of the specified route type.

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed OSPF routes in RIP.

Default Values

By default, this command is disabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 3.1	Command was introduced.

Functional Notes

Redistributing OSPF routes imports those routes into RIP without the interfaces in question actually participating in RIP. The OSPF routes imported this way are not covered by a network command and therefore do not send/receive RIP traffic.

If r**edistribute ospf** is enabled and no metric value is specified, the value defaults to **0**. The metric value defined using the **redistribute ospf metric** command overrides the **default-metric** command’s metric setting. Refer to the section *timeout-timer <seconds>* on page 1142 for more information.

Usage Examples

The following example imports OSPF routes into RIP:

```
(config)#router rip
(config-rip)#redistribute ospf
```

redistribute static [metric <*value*>]

Use the **redistribute static** command to pass routes from one network to another, regardless of the routing protocol implemented on the routing domain. Using the **static** keyword allows the propagation of static routes to other interfaces using the RIP routing protocol. Use the **no** form of this command to disable the propagation of the specified route type.

> NOTE *The gateway network for the static route must participate in RIP by using the network command for the gateway network.*

Syntax Description

metric <*value*>	Optional. Specifies the hop count to use for advertising redistributed OSPF routes in RIP.

.

Default Values

By default, RIP is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Functional Notes

Redistributing static routes allows other network devices to learn about paths (not compatible with their system) without requiring manual input to each device on the network.

timeout-timer *<seconds>*

Use the **timeout-timer** command to set the timeout timer value for a route when it is learned via RIP. Each time a RIP update for that route is received, the timeout timer is reset to this value. If no updates for that route are received in the specified number of seconds and the timeout timer expires, the route is considered invalid, and it will be removed from the route table. Use the **no** form of this command to return to the default settings.

Syntax Description

<seconds>	Sets the timeout-timer value. Valid range: 5 to 4294967295 seconds.

Default Values

By default, this value is set at 180 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

Note that the timeout timer value cannot be set to a value less than the **update-timer** value. It is recommended that this timer be set to a value that is three times the value of the **update-timer** (see *update-timer <seconds>* on page 1143.

Usage Examples

The following example configures the router to mark routes invalid if no RIP updates for those routes are received within 120 seconds.

```
(config)#router rip
(config-rip)#timeout-timer 120
```

update-timer *<seconds>*

Use the **update-timer** command to set the value of the RIP update interval timer. The RIP update interval is the number of seconds which must elapse between RIP update packet transmissions. Use the **no** form of this command to return to the default settings.

Syntax Description

<seconds>	Specifies the number of seconds allowed to elapse between RIP update packet transmissions. Valid range: 5 to 4294967295 seconds.

Default Values

By default, this value is set at 30 seconds.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Functional Notes

Note that the **timeout-timer** value cannot be set to a value less than the **update-timer** value. It is recommended that the **timeout-timer** be set to a value that is three times the value of the **update-timer**. (See *timeout-timer <seconds>* on page 1142 for more information.)

Usage Examples

The following example sets the rate at which RIP update messages are transmitted from the router to 20 seconds.

```
(config)#router rip
(config-rip)#update-timer 20
```

version [1 | 2]

Use the **version** command to specify (globally) the Routing Information Protocol (RIP) version used on all IP interfaces. This global configuration is overridden using the configuration commands **ip rip send version** and **ip rip receive version**. Use the **no** form of this command to return to the default value.

Syntax Description

1	Specifies RIP version 1 be used globally.
2	Specifies RIP version 2 be used globally.

Default Values

By default, RIP is not enabled.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 1.1	Command was introduced.

Usage Examples

The following example specifies RIP version 2 as the global RIP version:

```
(config)#router rip
(config-rip)#version 2
```

DHCP Pool Command Set

To activate the DHCP Pool mode, enter the **ip dhcp-server pool** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#ip dhcp-server pool MyPool
(config-dhcp)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

client-identifier <identifier> on page 1146

client-name <name> on page 1148

default-router <address> <secondary> on page 1149

dns-server <address> <secondary> on page 1150

domain-name <domain> on page 1151

hardware-address <hardware-address> <type> on page 1152

host <address> [<subnet mask> or <prefix length>] on page 1154

lease <days> <hours> <minutes> on page 1155

netbios-name-server <address> <secondary> on page 1156

netbios-node-type <type> on page 1157

network <address> [<subnet mask> or <prefix length>] on page 1158

ntp-server <ip address> on page 1159

option <option value> [ascii | hex | ip] <value> on page 1160

tftp-server <server> on page 1161

timezone-offset <offset> on page 1162

client-identifier *<identifier>*

Use the **client-identifier** command to specify a unique identifier (in dotted hexadecimal notation) for a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove a configured client identifier.

Syntax Description

<identifier>

Specifies a custom client identifier using a text string (that is converted to a hexadecimal equivalent) or 7 to 28 hexadecimal numbers (with colon delimiters).

OR

Specifies the hexadecimal Media Access Control (MAC) address including a hexadecimal number added to the front of the MAC address to identify the media type.

For example, specifying the **client-identifier** for a MAC address of d217.0491.1150 defines the client identifier as **01:d2:17:04:91:11:50** (where 01 defines the media type as Ethernet).

For example, a custom client identifier of **0f:ff:ff:ff:ff:51:04:99:a1** may be entered using the *<identifier>* option.

Default Values

client-id

By default, the client identifier is populated using the following formula:

TYPE: INTERFACE SPECIFIC INFO : MAC ADDRESS

Where TYPE specifies the media type in the form of one hexadecimal byte (refer to *hardware-address <hardware-address> <type>* on page 1152 for a detailed listing of media types) and MAC ADDRESS is the MAC address assigned to the first Ethernet interface in the unit in the form of six hexadecimal bytes. (For units with a single Ethernet interface, the MAC ADDRESS assigned to Ethernet 0/1 is used in this field).

INTERFACE SPECIFIC INFO is only used for Frame Relay interfaces and can be determined using the following:

FR_PORT# : Q.922 ADDRESS

Where the FR_PORT# specifies the label assigned to the virtual Frame Relay interface using four hexadecimal bytes. For example, a virtual Frame Relay interface labeled 1 would have a FR_PORT# of 00:00:00:01.

The Q.922 ADDRESS field is populated using the following:

8	7	6	5	4	3	2	1
DLCI (high order)						C/R	EA
DLCI (lower)				FECN	BECN	DE	EA

Where the FECN, BECN, C/R, DE, and high order EA bits are assumed
to be 0, and the lower order extended address (EA) bit is set to 1.

The following list provides a few example DLCIs and associated Q.922 addresses:

DLCI (decimal) / Q.922 address (hex)

16 / 0x0401
50 / 0x0C21
60 / 0x0CC1
70 / 0x1061
80 / 0x1401

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

DHCP clients use client identifiers in place of hardware addresses. To create the client-identifier, begin with the two-digit numerical code representing the media type and append the client's MAC address. For example, a Microsoft client with an Ethernet (01) MAC address d2:17:04:91:11:50 uses a client identifier of 01:d2:17:04:91:11:50.

Usage Examples

The following example specifies the client identifier for a Microsoft client with an Ethernet MAC address of **d217.0491.1150**:

```
(config)#ip dhcp-server pool Microsoft_Clients
(config-dhcp)#client-identifier 01:d2:17:04:91:11:50
```

client-name *<name>*

Use the **client-name** command to specify the name of a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured client name.

Syntax Description

<name>	Identifies the DHCP client (example is **client1**) using an alphanumeric string (up to 32 characters in length).

NOTE *The specified client name should not contain the domain name.*

Default Values

By default, there are no specified client names.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a client name of **myclient**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#client-name myclient
```

default-router *<address> <secondary>*

Use the **default-router** command to specify the default primary and secondary routers to use for the Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured router.

Syntax Description

<address>	Specifies the address (in dotted decimal notation) of the preferred router on the client's subnet (example: 192.22.4.254).
<secondary>	Optional. Specifies the address (in dotted decimal notation) of the second preferred router on the client's subnet (example: 192.22.4.253).

Default Values

By default, there are no specified default routers.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Functional Notes

When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCP client. The AOS allows a designation for two routers, listed in order of precedence.

Usage Examples

The following example configures a default router with address **192.22.4.253** and a secondary router with address **192.22.4.254**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#default-router 192.22.4.253 192.22.4.254
```

dns-server *<address> <secondary>*

Use the **dns-server** command to specify the default primary and secondary Domain Name System (DNS) servers to use for the Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured DNS server.

Syntax Description

<address>	Specifies the address (in dotted decimal notation) of the preferred DNS server on the network (example: 192.72.4.254).
<secondary>	Optional. Specifies the address (in dotted decimal notation) of the second preferred DNS server on the network (example: 192.100.4.253).

Default Values

By default, there are no specified default DNS servers.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a default DNS server with address **192.72.3.254** and a secondary DNS server with address **192.100.4.253**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#dns-server 192.72.3.254 192.100.4.253
```

domain-name *<domain>*

Use the **domain-name** command to specify the domain name for the Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured domain name.

Syntax Description

<name>	Identifies the DHCP client (e.g., adtran.com) using an alphanumeric string (up to 32 characters in length).

Default Values

By default, there are no specified domain names.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a domain name of **adtran.com**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#domain-name adtran.com
```

hardware-address *<hardware-address> <type>*

Use the **hardware-address** command to specify the name of a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured client name.

Syntax Description

<hardware-address> Specifies the hardware address (in hexadecimal notation with colon delimiters) of the preferred router on the client's subnet (example d2:17:04:91:11:50).

<type> Optional. Specifies the hardware protocol of the DHCP client.

The hardware type field can be entered as follows:

ethernet	Specifies standard Ethernet networks.
ieee802	Specifies IEEE 802 standard networks.
<1-21>	Enter one of the hardware types listed in RFC1700.

The valid hardware types are as follows:

1	10 Mb Ethernet
2	Experimental 3 Mb Ethernet
3	Amateur Radio AX.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNet)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transmission Mode (ATM)
20	Serial Line
21	Asynchronous Transmission Mode (ATM)

Default Values

By default, the hardware address type is set to 10 Mbps Ethernet.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies an Ethernet client with a MAC address of **ae:11:54:60:99:10**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#hardware-address ae:11:54:60:99:10 Ethernet
```

host *<address>* **[***<subnet mask>* or *<prefix length>***]**

Use the **host** command to specify the IP address and subnet mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to remove the configured client address.

Syntax Description

<address>	Specifies the IP address (in dotted decimal notation) for a manual binding to a DHCP client.
<subnet mask>	Optional. Specifies the network mask (subnet) for a manual binding to a DHCP client. If the subnet mask is left unspecified, the DHCP server examines its address pools to obtain an appropriate mask. If no valid mask is found in the address pools, the DHCP server uses the Class A, B, or C natural mask.
<prefix length>	Optional. Alternately, the prefix length may be used to specify the number of bits that comprise the network address. The prefix length must be preceded by a forward slash (/). For example, to specify an IP address with a subnet mask of 255.255.0.0, enter **/16** after the address.

Default Values

By default, there are no specified host addresses.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following examples show two different ways to specify a client with IP address **12.200.5.99** and a 21-bit subnet mask:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#host 12.200.5.99 255.255.248.0
```

or

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#host 12.200.5.99/21
```

lease *<days> <hours> <minutes>*

Use the **lease** command to specify the duration of the lease for an IP address assigned to a Dynamic Host Configuration Protocol (DHCP) client. Use the **no** form of this command to return to the default lease value.

Syntax Description

<days>	Specifies the duration of the IP address lease in days.
<hours>	Optional. Specifies the number of hours in a lease. You may only enter a value in the hours field if the days field is specified.
<minutes>	Optional. Specifies the number of minutes in a lease. You may only enter a value in the minutes field if the days and hours fields are specified.

Default Values

By default, an IP address lease is one day.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a lease of **2 days**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#lease 2
```

The following example specifies a lease of **1 hour**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#lease 0 1
```

The following example specifies a lease of **30 minutes**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#lease 0 0 30
```

netbios-name-server *<address> <secondary>*

Use the **netbios-name-server** command to specify the primary and secondary NetBIOS Windows Internet Naming Service (WINS) name servers available for use by the Dynamic Host Configuration Protocol (DHCP) clients. Use the **no** form of this command to remove a configured NetBIOS name server.

Syntax Description

<address>	Specifies the address (in dotted decimal notation) of the preferred NetBIOS WINS name server on the network (example: 192.72.4.254).
<secondary>	Optional. Specifies the address (in dotted decimal notation) of the second preferred NetBIOS WINS name server on the network (example: 192.100.4.253).

Default Values

By default, there are no configured NetBIOS WINS name servers.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a primary NetBIOS WINS name server with an IP address of **172.45.6.99** and a secondary with an IP address of **172.45.8.15**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#netbios-name-server 172.45.6.99 172.45.8.15
```

netbios-node-type *<type>*

Use the **netbios-node-type** command to specify the type of NetBIOS node used with Dynamic Host Configuration Protocol (DHCP) clients. Use the **no** form of this command to remove a configured NetBIOS node type.

Syntax Description

<type> Specifies the NetBIOS node type used with DHCP clients.

Valid node types are as follows:

b-node (1) - Broadcast node
p-node (2) - Peer-to-Peer node
m-node (4) - Mixed node
h-node (8) - Hybrid node (Recommended)

Alternately, the node type can be specified using the numerical value listed next to the nodes above.

Default Values

By default, the **netbios-node-type** is set to **h-node** (8) - Hybrid node.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following example specifies a client's NetBIOS node type as **h-node**:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#netbios-node-type h-node
```

Alternately, the following also specifies the client's NetBIOS node type as **h-node**:

```
(config-dhcp)#netbios-node-type 8
```

network *<address>* **[***<subnet mask>* or *<prefix length>***]**

Use the **network** command to specify the subnet number and mask for an AOS Dynamic Host Configuration Protocol (DHCP) server address pool. Use the **no** form of this command to remove a configured subnet.

Syntax Description

<ip address>	Specifies the IP address (in dotted decimal notation) of the DHCP address pool.
<subnet mask>	Optional. Specifies the network mask (subnet) for the address pool. If the subnet mask is left unspecified, the DHCP server uses the Class A, B, or C natural mask.
<prefix length>	Optional. Alternately, the prefix length may be used to specify the number of bits that comprise the network address. The prefix length must be preceded by a forward slash (/). For example, to specify an IP address with a subnet mask of 255.255.0.0, enter **/16** after the address.

Default Values

By default, there are no configured DHCP address pools.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 2.1	Command was introduced.

Usage Examples

The following examples show two different ways to configure an address pool subnet of **192.34.0.0** with a 16-bit subnet mask:

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#network 192.34.0.0 255.255.0.0
```

or

```
(config)#ip dhcp-server pool MyPool
(config-dhcp)#network 192.34.0.0 /16
```

ntp-server *<ip address>*

Use the **ntp-server** command to specify the name of the Network Time Protocol (NTP) server published to the client.

Syntax Description

<ip address>	Specifies the IP address of the NTP server.

Default Values

By default, no NTP server is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example specifies the IP address of the NTP server:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#ntp-server 192.168.1.1
```

option *<option value>* [ascii | hex | ip] *<value>*

Use the **option** command to describe a generic DHCP option to be published to the client. The user may specify any number of generic options to be published to the client.

Syntax Description

<option value>	Specifies the value of the generic DHCP option published to the client. Range: 0 to 255.
ascii	Specifies the DHCP option information in ascii format.
hex	Specifies the DHCP option information in hexidecimal format.
ip	Specifies the DHCP option information in IP format.
<value>	Specifies the ASCII, hexidecimal, or IP value. The value for **ascii** is simple text. The value for **hex** is an 8-digit hexidecimal number (32 bit). The value for **ip** is a standard IP address in the format A.B.C.D.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example publishes DHCP options to the client:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#option 100 ascii ascii_value
(config-dhcp)#option 101 hex AB458E80
(config-dhcp)#option 102 ip 192.168.1.1
```

tftp-server *<server>*

Use the **tftp-server** command to specify the IP address or DNS name of the TFTP server published to the client.

Syntax Description

<server>	Specifies the DNS name or dotted notation IP address of the server.

Default Values

By default, no tftp server is defined.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example specifies the IP address of the TFTP server:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#tftp-server 192.168.1.1
```

The following example specifies the DNS name of the TFTP server:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#tftp-server MyServer.adtran.com
```

timezone-offset *<offset>*

Use the **timezone-offset** command to specify the timezone adjustment (in hours) published to the client.

Syntax Description

<offset>	Specifies the timezone adjustment (in hours) published to the client. Use an integer from -12 to 12.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.

Usage Examples

The following example sets the timezone adjustment for the client to -3 hours. For example, if the server time is configured for eastern time and the client is configured for Pacific time, you can set the client timezone adjustment to -3 hours:

```
(config)#ip dhcp pool MyPool
(config-dhcp)#timezone-offset -3
```

QUALITY OF SERVICE (QOS) MAP COMMANDS

A QoS policy is defined using a QoS map in the AOS CLI. The QoS map is a named list with sequenced entries. An entry contains a single match reference and one or more actions (priority, set, or both). To activate the QoS Command Set (which allows you to create and/or edit a map), enter a valid version of the QoS command at the Global Configuration mode prompt. Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign match order.

Once created, a QoS map must be applied to an interface (using the **qos-policy out** <*map-name*> command) in order to actively process traffic. Any traffic for the interface that is not sent to the priority queue is sent using the default queuing method for the interface (such as weighted fair queuing).

For example:

```
>enable
#config terminal
(config)#qos map VOICEMAP 10
(config-qos-map)#match precedence 5
(config-qos-map)#priority 512
(config-qos-map)#exit
(config)#interface fr 1
(config-fr 1)#qos-policy out VOICEMAP
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

bandwidth [percent | remaining | <value>] on page 1164

match on page 1165

priority on page 1166

set dscp <0-63> on page 1167

set precedence <0-7> on page 1168

bandwidth [percent | remaining | <*value*>]

Use the **bandwidth** command to provide the bandwidth value of an interface to the higher-level protocols. This value is used in cost calculations. Use the **no** form of this command to restore the default values.

Syntax Description

percent	Specifies percent of total interface bandwidth.
remaining	Specifies percent of total interface bandwidth minus any priority entry bandwidth values on this QOS map.
<*value*>	Specifies the bandwidth value in kbps. Valid range is from 8 to 2000000

Default Values

By default, there is no bandwidth configured for a QOS map entry.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 9.1	Command was introduced.
Release 10.0	New subcommands **percent** and **remaining** were added.

Functional Notes

When configuring entries within a QOS map set in Rev. 10, there are a few rules to be aware of:

1. The units of the bandwidth (kbps, percent, or remaining percent) must be consistent for all class-based entries (use the **bandwidth** command) in a QOS map set.
2. The total bandwidth between all priority entries and class-based entries in a QOS map set should not be configured beyond 75 percent of the bandwidth on the interface that the qos-policy is applied to, or the map will not be used.
3. Up to four class-based entries can be configured on a particular QOS map set that is applied to an interface. Up to sixteen class-based entries can be configured in the box (four entries on four QOS maps).

Usage Examples

The following example sets bandwidth of the QoS map to 10 Mbps:

```
(config)#qos map 1
(config-qos-map 1)#bandwidth 10000
```

match

Use the **match** command to specify which traffic should be processed by this QoS map. Possible variations of this command include:

match dscp *<0-63>*
match ip rtp *<port #>*
match ip rtp *<first port # in range> <last port # in range>*
match ip rtp *<first port # in range> <last port # in range>* **all**
match list *<listname>*
match precedence *<0-7>*
match protocol bridge
match protocol bridge netbeui

Syntax Description

dscp *<0-63>*	Matches IP packets with the specified DSCP value.
ip rtp *<start><end>* **all**	Matches RTP packets with even UDP destination port numbers in the specified range (between start and end). If **all** (which is optional) is specified, even and odd ports are matched in the specified range.
list *<listname>*	Specifies the name of the access-list (ACL) you wish to use to match packets for this QoS map. Refer to *ip access-list extended <listname>* on page 344 for more information on creating access-lists.
precedence *<0-7>*	Matches IP packets with the specified IP precedence value.
protocol bridge	Matches frames being bridged by the router.
protocol bridge netbeui	Matches only NetBEUI frames being bridged by the router.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

The following example assigns a traffic match pattern to the existing QoS map VOICEMAP:

```
(config)#qos map VOICEMAP 10
(config-qos-map)#match ip rtp 16384 20000
```

priority

The **priority** command provides a high-priority queue, prioritizing this traffic above all others. If no traffic is present in any other queue, priority traffic is allowed to burst up to the interface rate; otherwise, priority traffic above the specified bandwidth is dropped. Use the **no** form of this command to disable this feature.

Variations of this command include:

priority *<bandwidth>*
priority *<bandwidth> <burst>*
priority unlimited

Syntax Description

<bandwidth>	Specifies the permitted priority queue bandwidth in kilobits per second. This sets an upper limit for how much bandwidth is reserved for priority traffic.
<burst>	Optional. Specifies the burst size (in bytes) for traffic in this priority queue. This parameter should be left unconfigured for optimal performance.
unlimited	Optional. Specifies no limits on the priority queue bandwidth.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

This example assigns the matched traffic to a high priority output queue for any assigned interface:

```
(config)#qos map VOICEMAP 10
(config-qos-map)#match ip rtp 16384 20000
(config-qos-map)#priority 512
```

set dscp *<0-63>*

The **set dscp** command is an optional command for a QoS map that can be used to modify the DSCP field (on matching packets) to the specified value.

Syntax Description

<0-63>	Specifies the decimal DSCP value.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

This command sets the DSCP value (for all matching traffic) to 46:

```
(config)#qos map VOICEMAP 10
(config-qos-map)#set dscp 46
```

set precedence *<0-7>*

The **set precedence** command is an optional command for a QoS map that can be used to modify the IP precedence value (on matching packets) to the specified value.

Syntax Description

<0-7>	Specifies the decimal IP precedence value.

Default Values

No default value is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 6.1	Command was introduced.

Usage Examples

This command sets the IP precedence value (for all matching traffic) to 5:

```
(config)#qos map VOICEMAP 10
(config-qos-map)#set precedence 5
```

RADIUS GROUP COMMAND SET

To activate the Radius Group mode, enter the **aaa group server** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#aaa group server radius myServer
(config-sg-radius)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

cross-connect <#> <from interface> <slot/port> <tdm-group#> <to interface> <slot/port> on page 28

description <text> on page 31

do on page 32

end on page 33

exit on page 34

shutdown on page 35

All other commands for this command set are described in this section in alphabetical order.

server [acct-port <port number>| auth-port <port number>] on page 1170

server [acct-port *<port number>*| auth-port *<port number>*]

Use the **server** command to add a predefined RADIUS server to the current named list of servers. See *radius-server* on page 436 for more information.

Syntax Description

acct-port *<port number>*	Defines the accounting port value.
auth-port *<port number>*	Defines the authorization port value.

Default Values

No defaults necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 5.1	Command was introduced.

Usage Examples

The following example adds a server to the **myServers** list:

```
(config)#aaa group server radius myServers
(config-sg-radius)#server 1.2.3.4 acct-port 786 auth-port 1812
(config-sg-radius)#server 4.3.2.1
(config-sg-radius)#exit
(config)#
```

or

```
(config)#aaa group server radius myServers
(config-sg-radius)#server 4.3.2.1
(config-sg-radius)#exit
(config)#
```

ROUTE MAP COMMAND SET

To activate the Route Map Interface Configuration mode, enter the **route-map** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#route-map MyMap permit 100
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 32

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

match as-path <name> on page 1172

match community <name> [exact-match] on page 1173

match ip address <access list name> on page 1174

match ip address prefix-list <prefix-list name> on page 1175

match ip dscp [<value> | afxx | csxx | default | ef] on page 1176

match ip precedence [<value> | critical | flash | flash-override | immediate | internet | network | priority | routine] on page 1177

match metric <value> on page 1178

match length <minimum> <maximum> on page 1179

set as-path prepend [<number> | last-as <number>] on page 1180

set comm-list <name> delete on page 1181

set local-preference <value> on page 1182

set metric <value> on page 1183

set default interface <interface type> <interface id> on page 1184

set interface <interface type> <interface id> on page 1185

set ip default next-hop <ip address> on page 1186

set ip df on page 1187

set ip dscp [<value> | afxx | csxx | default | ef] on page 1188

set ip next-hop <ip address> on page 1189

set ip precedence [<value> | critical | flash | flash-override | immediate | internet | network | priority | routine] on page 1190

match as-path *<name>*

Use the **match as-path** command to configure the route map to route traffic based on the AS path list name. Use the **no** form of this command to discontinue matching.

Syntax Description

<name>	Specifies the name of the AS path list you want to match.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the AS path list named **TestPath**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match as-path TestPath
```

match community *<name>* [exact-match]

Use the **match community** command to configure the route map to route traffic based on a specified community. Use the **no** form of this command to discontinue matching.

Syntax Description

<name>	Specifies the name of the community you want to match.
exact-match	Optional. Specifies that the route map must match the community name exactly.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the community named **MyCommunity**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match community MyCommunity
```

match ip address *<access list name>*

Use the **match ip address** command to configure the route map to route traffic based on the access list name defined with the **ip access-list** command. Refer to *ip access-list extended <listname>* on page 344 for more information. Use the **no** form of this command to discontinue matching.

Syntax Description

<access list name>	Specifies the name of the access list to match.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the IP address access list named **MyList**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match ip address MyList
```

match ip address prefix-list *<prefix-list name>*

Use the **match ip address prefix-list** command to configure the route map to route traffic based on a prefix list route filter. The name of the prefix list is defined with the **ip prefix-list** command. Refer to *ip prefix-list <listname> description <"text">* on page 397 for more information. Use the **no** form of this command to discontinue matching.

Syntax Description

<prefix-list name>	Specifies matching the IP address based on the prefix list name.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the IP address prefix list named **MyList**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match ip address prefix-list MyList
```

match ip dscp [<*value*> | af*xx* | cs*xx* | default | ef]

Use the **match ip dscp** command to configure the route map to route traffic based on the Differentiated Services Code Point (DSCP) value in the IP header of the packet. Use the **no** form of this command to discontinue matching.

Syntax Description

<*value*>	Specifies the DSCP numeric value to match. (Valid range: 0 to 63.)
afxx	Specifies the assured forwarding (AF) value to match. (Select from: 11, 12, 13, 21, 22, 23, 31, 32, 33, 41, 42, or 43.)
csxx	Specifies the class selector (CS) value to match. (Valid range: 1 to 7.)
default	Specifies matching the default IP DSCP value.
ef	Specifies matching those packets marked for expedited forwarding (EF).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the IP header with a DSCP AF value of **11**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match ip dscp af11
```

match ip precedence [*<value>* | critical | flash | flash-override | immediate | internet | network | priority | routine]

Use the **match ip precedence** command to configure the route map to route traffic based on the precedence value in the IP header of the packet. Use the **no** form of this command to discontinue matching.

Syntax Description

<value>	Specifies matching the IP precedence (in numeric value). (Valid range: 0 to 7 in ascending order of importance.)
routine	Specifies matching the IP precedence **routine**. (Numeric value of 0.)
priority	Specifies matching the IP precedence **priority**. (Numeric value of 1.)
immediate	Specifies matching the IP precedence **immediate**. (Numeric value of 2.)
flash	Specifies matching the IP precedence **flash**. (Numeric value of 3.)
flash-override	Specifies matching the IP precedence **flash-override**. (Numeric value of 4.)
critical	Specifies matching the IP precedence **critical**. (Numeric value of 5.)
internet	Specifies matching the IP precedence **internet**. (Numeric value of 6.) This level is reserved for internal network use.
network	Specifies matching the IP precedence **network**. (Numeric value of 7.) This level is reserved for internal network use.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the IP precedence value of **critical**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match ip precedence critical
```

match metric *<value>*

Use the **match metric** command to configure the route map to route traffic based on a specified metric value. Use the **no** form of this command to discontinue matching.

Syntax Description

<value>	Specifies the metric value you want to match. (Valid range: 1 to 4,294,967,295.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match the metric value **100**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match metric 100
```

match length *<minimum> <maximum>*

Use the **match length** command to configure the route map to route traffic based on the packet length. Use the **no** form of this command to discontinue matching.

Syntax Description

<minimum>	Specifies the minimum packet length you want to match. (Valid range: 1 to 4,294,967,295.)
<maximum>	Specifies the maximum packet length you want to match. (Valid range: 1 to 4,294,967,295.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example instructs the route map named **MyMap** to match packets with a minimum length of **1** and a maximum length of **200**:

```
(config)#route-map MyMap permit 100
(config-route-map)#match length 1 200
```

set as-path prepend [<*number*> | last-as <*number*>]

Use the **set as-path prepend** command to prepend a number to the AS path to influence the best-path selection process by making the AS path appear further away. Use the **no** form of this command to disable this feature.

Syntax Description

as-path prepend <*number*>	Specifies a number to be prepended to the AS path value as an autonomous number. (Valid range: 1 to 65,535.)
as-path prepend last-as <*number*>	Specifies a number to be prepended to the last AS path number. (Valid range: 1 to 10.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example prepends the number **2** to the last AS path number:

```
(config)#route-map MyMap permit 100
(config-route-map)#set as-path prepend last-as 2
```

set comm-list *<name>* delete

Use the **set comm-list delete** command to specify a list of communities to delete. Use the **no** form of this command to disable this feature.

Syntax Description

<name>	Specifies the name of the list of communities to delete.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example deletes the community list named **listname**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set comm-list listname delete
```

set local-preference *<value>*

Use the **set local-preference** command to restrict traffic to a local autonomous system. Use the **no** form of this command to cancel the local preference.

Syntax Description

<value>	Sets the local preference value. (Valid range: 0 to 4,294,967,295.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the local preference fro **MyMap** to a value of **100**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set local-preference 100
```

set metric *<value>*

Use the **set metric** command to specify a metric value for the route map. Use the **no** form of this command to cancel the metric value.

Syntax Description

<value>	Sets the metric value. (Valid range: 0 to 4,294,967,295.)

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000R, 2000, 3000, 4000, and 5000 Series and Total Access 900 Series units.

Command History

Release 10.1	Command was introduced.

Usage Examples

The following example sets the metric value for **MyMap** to **100**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set metric 100
```

set default interface *<interface type> <interface id>*

Use the **set default interface** command to specify an output interface for the packet if there is no explicit route destination. Multiple interfaces can be specified but they must be point-to-point. The router forwards the packet along the first usable interface. Use the **no** form of this command to cancel output from the specified interface.

Syntax Description

<interface>	Sets default interface type. Type **set default interface ?** for a list of valid interfaces.
<interface id>	Specifies the ID of the specified interface type.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the default interface as PPP 1:

```
(config)#route-map MyMap permit 100
(config-route-map)#set default interface ppp 1
```

set interface *<interface type> <interface id>*

Use the **set interface** command to specify an output interface for the packet. Multiple interfaces can be specified. The router forwards the packet along the first usable interface. Use the **no** form of this command to cancel output from the specified interface.

Syntax Description

<interface>	Sets output interface type for the packet. Type **set interface ?** for a list of valid interfaces.
<interface id>	Specifies the ID of the specified interface type.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the output interface as PPP 1:

```
(config)#route-map MyMap permit 100
(config-route-map)#set interface ppp 1
```

set ip default next-hop *<ip address>*

Use the **set ip default next-hop** command to specify an IP address for the next hop if there is no explicit route destination. The default next hop is used if no specific route to the destination has been defined. Use the **no** form of this command to cancel the default next hop.

Syntax Description

<ip address>	Specifies the default IP address for the next hop.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the default interface for the next hop as **10.10.11.254**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set ip default next-hop 10.10.11.254
```

set ip df

Use the **set ip df** command to identify the packet as “don’t fragment” (DF). Use the **no** form of this command to remove this designation.

Syntax Description

No subcommands.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example designates the packet as “don’t fragment”:

```
(config)#route-map MyMap permit 100
(config-route-map)#set ip df
```

set ip dscp [<*value*> | **af**xx | **cs**xx | default | ef]

Use the **set ip dscp** command to set the Differentiated Services Code Point (DSCP) value in the IP header of the packet. Use the **no** form of this command to discontinue matching.

Syntax Description

<*value*>	Sets the DSCP numeric value. (Valid range: 0 to 63.)
afxx	Sets the assured forwarding (AF) value. (Select from: 11, 12, 13, 21, 22, 23, 31, 32, 33, 41, 42, or 43.)
csxx	Sets the class selector (CS) value. (Valid range: 1 to 7.)
default	Sets the default IP DSCP value.
ef	Marks the packet for expedited forwarding (EF).

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets a DSCP value of **af11** in the IP header of the route map named **MyMap**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set ip dscp af11
```

set ip next-hop *<ip address>*

Use the **set ip next-hop** command to specify the interface for the next hop. Multiple IP addresses can be specified. The packet is forwarded along the first usable IP address. Use the **no** form of this command to cancel the next hop.

Syntax Description

<ip address>	Specifies the IP address for the next hop.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets the next hop IP address as **10.10.11.254** in the header of the route map named **MyMap**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set ip next-hop 10.10.11.254
```

set ip precedence [<*value*> | critical | flash | flash-override | immediate | internet | network | priority | routine]

Use the **set ip precedence** command to set the precedence value in the IP header of the packet. Use the **no** form of this command to remove the precedence value.

Syntax Description

<*value*>	Sets the IP precedence (in numeric value). (Valid range: 0 to 7 in ascending order of importance.)
routine	Sets the IP precedence as **routine**. (Numeric value of 0.)
priority	Sets the IP precedence as **priority**. (Numeric value of 1.)
immediate	Sets the IP precedence as **immediate**. (Numeric value of 2.)
flash	Sets the IP precedence as **flash**. (Numeric value of 3.)
flash-override	Sets the IP precedence as **flash-override**. (Numeric value of 4.)
critical	Sets the IP precedence as **critical**. (Numeric value of 5.)
internet	Sets the IP precedence as **internet**. (Numeric value of 6.) This level is reserved for internal network use.
network	Sets the IP precedence as **network**. (Numeric value of 7.) This level is reserved for internal network use.

Default Values

No default value necessary for this command.

Applicable Platforms

This command applies to the NetVanta 2000 and 5000 Series, and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example sets an IP precedence value of **critical** in the IP header of the route map named **MyMap**:

```
(config)#route-map MyMap permit 100
(config-route-map)#set ip precedence critical
```

TACACS+ Group Configuration Command Set

To activate the Terminal Access Controller Access Control System Plus (TACACS+) Group Configuration mode, enter the **aaa group server tacacs+** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#aaa group server tacacs+ TEST GROUP
(config-sg-tacacs+)#
```

The following commands are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the sections listed below:

do on page 32

end on page 33

exit on page 34

All other commands for this command set are described in this section in alphabetical order.

server <host> on page 1192

server *<host>*

Use the **server** command to specify a particular TACACS+ server's IP address or host name.

Syntax Description

<host>	Specifies a TACACS+ server IP address.

Default Values

No default is necessary for this command.

Applicable Platforms

This command applies to the NetVanta 300, 1000, 1000R, 2000, 3000, 4000, and 5000 and Total Access 900 Series units.

Command History

Release 11.1	Command was introduced.

Usage Examples

The following example specifies the IP address of the TACACS+ server:

```
(config)#aaa group server tacacs+ TEST_GROUP
(config-sg-tacacs+)#server 192.168.1.1
(config-sg-tacacs+)#
```

Index